UNIVERSIDADE FEDERAL DE SANTA CATARINA
INFORMÁTICA E ESTATÍSTICA

Felipe Coral Sasso

CARTÃO DE IDENTIFICAÇÃO HUMANA PARA AUTENTICAÇÃO E AUTORIZAÇÃO SEGURA

Florianópolis

2016

Felipe Coral Sasso

CARTÃO DE IDENTIFICAÇÃO HUMANA PARA AUTENTICAÇÃO E AUTORIZAÇÃO SEGURA

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do Grau de Mestre em Ciência da Computação.
Orientador: Prof. Ricardo Alexandre Reinaldo de Moraes, Dr.
Coorientador: Prof. Jean Everson Martina, Dr.

Florianópolis

2016

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Sasso, Felipe
Cartão de Identificação humana para autenticação e autorização segura / Felipe Sasso ; orientador, Ricardo Moraes ; coorientador, Jean Martina. - Florianópolis, SC, 2016.
100 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da Computação. 2. Federação. 3. Gerenciamento de Identidade. 4. Dados Biométricos. 5. ICAO 9303. I. Moraes, Ricardo. II. Martina, Jean. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. IV. Título.

Felipe Coral Sasso

CARTÃO DE IDENTIFICAÇÃO HUMANA PARA AUTENTICAÇÃO E AUTORIZAÇÃO SEGURA

Esta Dissertação foi julgada aprovada para a obtenção do Título de "Mestre em Ciência da Computação", e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Florianópolis, 11 de fevereiro 2016.

Profª. Carina Friedrich Dorneles, Drª.
Coordenadora do Curso

Prof. Jean Everson Martina, Dr.
Coorientador

Banca Examinadora:

Prof. Ricardo Alexandre Reinaldo de Moraes, Dr.
Orientador

Profª. Natalia Castro Fernandes, Drª.
Universidade Federal Fluminense

Prof. Mario Antônio Ribeiro Dantas, Dr.
Universidade Federal de Santa Catarina

Prof. Ricardo Felipe Custódio, Dr.
Universidade Federal de Santa Catarina

Dedico este trabalho aos meus pais, familiares e amigos. Em especial ao meu avô que nos deixou pouco antes da finalização deste trabalho.

AGRADECIMENTOS

Gostaria de agradecer aqui a todos que, de uma forma ou de outra, foram fundamentais nessa etapa da minha vida.

Primeiramente, gostaria de agradecer aos meus pais, meus avós e meus irmãos por todo apoio que deram nesta jornada.

Gostaria também de agradecer a Thaís por estar ao meu lado sempre, nos momentos de alegria e angústia e por me ajudar a vencer cada desafio encontrado no caminho. Seu companheirismo foi fundamental no decorrer de mais essa etapa.

Um agradecimento especial à todos os amigos que fiz no LabSEC. Principalmente os parceiros do dia a dia no café da tarde nas lanchonetes aos arredores do LabSEC, ou naquele maravilhoso quibe no Restaurante Universitário.

Por fim mas não menos importante, agradeço ao meu orientador Ricardo Alexandre Reinaldo de Moraes, coorientador Jean Everson Martina que me guiaram durante o desenvolvimento deste trabalho.

A persistência é o caminho do êxito

Charles Chaplin

RESUMO

Vários esforços tem sido feitos recentemente no âmbito de federações de identidade. Os esforços para que dados de autenticação sejam disponíveis e utilizáveis por todas as entidades participantes da federação são o pilar deste modelo. No entanto alguns problemas se encontram em aberto. O primeiro deles é o funcionamento *offline* do processo de autenticação. Hoje o modelo da federação requer que os sistemas trabalhem *online* de forma síncrona, o que limita seu uso para algumas aplicações. Segundo, os dados da federação somente estão disponíveis para sistemas computacionais e não para as pessoas, tornando difícil a avaliação de tais credenciais. Por fim, a federação tem inúmeros problemas técnicos e legais para a disponibilização de dados considerados de uso privados, tais como biométricos. Estes tornariam a autenticação muito mais forte. A proposta desta dissertação foi descrever um cartão de identificação baseado no padrão ICAO 9303 que soluciona os problemas presentes nas Federações de Identidade. Além da criação do cartão, também foi realizado uma avaliação da segurança deste em diversos cenários de uso. Com isso foi possível identificar quais problemas de segurança podem ocorrer durante a utilização do cartão e como resolvê-los.

Palavras-chave: Federação. Gerenciamento de Identidade. Documentos Digitais. Dados Biométricos. ICAO 9303

ABSTRACT

Several efforts have been made recently to establish identity federations. Efforts towards availability of authentication data to be usable by all entities of the federation are the core of this model. However some issues are still open. The first issue is related to offline operation of the authentication process. Today's model of federation requires that systems work online and synchronously, which limits the use for some applications. The second is related to the fact that data federations are only to computer systems and not by human agents. Thus it is difficult for humans involved in the process to assess such credentials. Finally, federation has numerous technical and legal issues for the provision of private data, such as biometric parameters, and it would make a much stronger authentication process. The purpose of this thesis is to describe an identity card based on the ICAO 9303 standard to solve the problems present in Identity Federations. Besides the creation of the card we also performed an evaluation of the Security in various usage scenarios. It was possible to identify which security issues may arise during the use of the card and how to solve them.

Keywords: Federations. Identity Management. Digital Documents. Biometric Data. ICAO 9303

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 CONTEXTUALIZAÇÃO

O uso de redes de computadores, em particular quando se utiliza a Internet para acesso a serviços remotos, trouxe a necessidade de criação de uma base de dados com informações sobre pessoas. Essa demanda de reconhecimento e validação de acesso dos usuários aos serviços pode ser sintetizada em duas etapas: autenticação e autorização (MOREIRA et al., 2011). O cumprimento dessas etapas implica na necessidade de manutenção da base de dados com registros sobre os usuários do serviço. Para quem disponibiliza o serviço é necessário criar e manter suas próprias bases de dados e para quem os utiliza, é preciso criar e manter contas para cada serviço que se deseja o acesso. Para facilitar a demanda dessas aplicações foram criadas as federações de identidade. Conforme visto em Moreira et al. (2011), uma federação de identidade visa minimizar as demandas dos provedores e dos usuários de serviços disponibilizados por instituições. A ideia é que as informações de identificação de um usuário sejam mantidas e gerenciadas pelas instituições no qual um usuário possui algum tipo de ligação.

O uso de federações de identidade como um método de integrar a autenticação é uma realidade em diversos ambientes, como por exemplo, ambientes acadêmicos. Neste contexto, cada instituição participante da federação pode disponibilizar as credenciais de um usuário. Essas credenciais podem ser usadas em serviços oferecidos pela federação, tirando de cada sistema a responsabilidade de armazená-las. Então, quando um acadêmico visita outra instituição, ele pode usar os serviços oferecidos pela instituição visitada apenas apresentando suas credenciais de autenticação de sua instituição de origem, criando assim o princípio de identidade federada (MOREIRA et al., 2011).

Uma federação de identidade consiste em duas entidades: Provedores de Identidades (IdP) , que são responsáveis por gerenciar as credenciais de autenticação de usuários e suas informações pessoais, e os Provedor de Serviços (SP), que oferecem serviços que estes usuários podem utilizar através das credenciais do IdP (BALDONI, 2012). Assim, serviços não precisam manter informações de usuários e estes não precisam memorizar diversas informações de autenticação, como os tradicionais *login* e senha. Entretanto, observa-se alguns problemas neste modelo. O principal deles é que as federações requerem que provedores de serviços e identidades estejam disponíveis *online*, ou seja, o provedor de identidade e a instituição origem precisam de alguma forma se comunicarem para que os usuários possam acessar um

dado serviço. Ademais, as identidades providas pela federação requerem o uso de computadores para sua verificação, restringindo o seu uso ao contexto de sistemas computacionais, dificultando a verificação por agentes humanos. Porém, o uso de credenciais verificáveis por agentes humanos pode ajudar em vários cenários onde a identificação é ordinária e necessária. Um exemplo é o requerimento de identificação para descontos em cinemas e teatros. Além disso, em algumas aplicações, tais como empréstimos de livros ou acesso a alguns ambientes físicos de uso compartilhado, pode não ser necessário uma verificação *online*.

Uma outra importante questão é que alguns dados são considerados privados, confidenciais e de uso restrito. Neste sentido, a instituição de origem não pode compartilhá-los através de seu provedor de identidade, pois, caso ocorra o seu vazamento, a instituição pode sofrer sanções legais por quebra de privacidade. Um exemplo de uso de um dado privado é a informação biométrica em um processo de autenticação. Esse tipo de dado pode ser útil como um segundo fator de autenticação, mas sua coleta, armazenamento e transmissão são muito sensíveis a problemas de privacidade em atividades dentro de uma federação.

Encontra-se, na literatura, diversos desafios tecnológicos para o uso de federações de identidade. De uma forma não extensiva, destacam-se:

- Segurança: Os principais problemas são o roubo de identidade, mau uso de atributos e comprometimento de dados sigilosos, como visto em Bhargav-Spantzel, Squicciarini e Bertino (2005); Ahn e Lam (2005); Ahn, Shin e Hong (2004); Bertino et al. (2010); Han et al. (2010); Landau, Gong e Wilton (2009); Madsen, Koga e Takahashi (2005); Maler e Reed (2008);

- Privacidade: Apresentam-se na literatura algumas preocupações de privacidade devido a grande troca de informações sensíveis de identidade através de fronteiras organizacionais, vistos em Ahn e Lam (2005); Ahn, Shin e Hong (2004); Bertino et al. (2010); Glasser e Vajihollahi (2008); Landau, Gong e Wilton (2009); Maler e Reed (2008); Shin, Lopes e Claycomb (2009); Bhargav-Spantzel, Squicciarini e Bertino (2005);

- Interoperabilidade: Há situações em que os parceiros aderem a padrões diferentes, e isso aumenta a complexidade, apresentado em Bertino et al. (2010); Maler e Reed (2008); Speltens e Patterson (2007); Wolf et al. (2009).

Entende-se que para resolver esses problemas é necessário um método que atenda aos seguintes requisitos:

- Requisito 1: O usuário deve carregar suas credenciais, de forma que não seja necessário a guarda *online* dados de identificação do mesmo;

- Requisito 2: O usuário pode manter seus dados privados, permitindo o acesso a esses apenas com seu consentimento. Um exemplo de dado privado são os dados biométricos de cada indivíduo;

- Requisito 3: O usuário pode agir como seu próprio Provedor de Identidade, tanto para acesso a serviços *online* quanto acesso a serviços *offline* (como catraca de ônibus, cara-crachá, entre outros).

Dessa forma, é necessário a concepção de um método de autenticação *offline* e que minimize a necessidade de comunicação *online* entre as instituições participantes. Também é desejável, em algumas situações que agentes humanos possam verificar identidades sem a utilização de computadores. Por fim, é essencial que o usuário controle seus dados privados (e.g. informações biométricas) e como estas informações são salvas, transmitidas e usadas.

O foco deste trabalho de pesquisa está na proposição de um cartão de identificação e a principal hipótese de pesquisa é que o padrão utilizado atualmente na confecção de passaportes pode resolver estes problemas presentes no âmbito de federações de identidade. Este padrão foi especificado pela Organização de Aviação Civil Internacional (ICAO) e estabelecido pela série de documentos 9303 (ICAO, 2014). Por ser o padrão utilizado em passaportes, já é bem compreendido, tanto em termos de software quanto em termos de requisitos de hardware. Este formato representa as credenciais de uma forma que garante a segurança e autenticidade destas. Com este padrão, é possível ter credenciais não tão sensíveis como nome e data de nascimento impressos no documento, podendo ser lidos por humanos ou por máquinas. Além disso, os dados sensíveis podem ser salvos no passaporte em um circuito integrado sem contato de forma segura, possibilitando uma verificação, por exemplo, das digitais do portador sem que as mesmas trafeguem através da Internet. Uma vez que estes dados podem ser assinados digitalmente pelo país emissor do passaporte, tem-se uma garantia da sua autenticidade. A ICAO 9303 detalha especificações como dados obrigatórios e opcionais que precisam estar nos documentos, como acessá-los

e como verificar a sua autenticidade. Além disso, o padrão especifica diferentes níveis de serviços, incluindo documentos com armazenamento de dados. Neste, informações biométricas como impressão digital e íris podem ser armazenadas de forma segura.

1.1 OBJETIVO GERAL

O objetivo principal desta dissertação é desenvolver e avaliar um método para a criação de um cartão de identificação que permita a autenticação *offline*, a avaliação das credenciais por um agente humano (sem o uso de computador), que faça uso de dados biométricos privados de maneira segura e que possa ser utilizado para emissão de certificados digitais sem a necessidade de uma nova verificação dos dados biométricos. O método proposto será direcionado para ambientes federados.

1.1.1 Objetivos específicos

Os objetivos específicos deste trabalho são:

- Realizar um estudo do estado da arte sobre federações de identidade;
- Propor um padrão de cartão de identificação humana para utilização no âmbito das Federações de Identidade;
- Avaliar a segurança do cartão proposto utilizando cerimônias;
- Descrever usos do cartão de identificação.

1.2 JUSTIFICATIVA

Atualmente, o uso de federações de identidade para integração de autenticação é uma realidade, que está em constante desenvolvimento. Entretanto, ainda há muito a ser estudado em questões relacionadas com problemas como roubo de identidade, comprometimento e privacidade de dados e interoperabilidade. Alguns estudos feitos por Bhargav-Spantzel, Squicciarini e Bertino (2005), Ahn e Lam (2005) e Bertino et al. (2010) ajudam a entender cada um desses problemas. Uma forma de resolver esses problemas seria o portador carregar consigo seus dados de forma segura, incluindo os dados mais sensíveis, e.g. as impressões digitais. Desta forma, consegue-se evitar que os diversos dados dos usuários trafeguem várias vezes através da Internet.

A viabilidade de implementação seria armazenar os dados em um cartão, onde o portador poderia transportá-lo e utilizá-lo como um cartão de identificação no âmbito das federações. O padrão dos passaportes apresentado pela ICAO atende bem esses requisitos de segurança, uma vez que os dados podem ser seguramente armazenados. Além do armazenamento seguro, a ICAO também descreve como os dados podem ser impressos, possibilitando a leitura tanto por agentes humanos quanto por máquinas.

Apesar do padrão ICAO ser o que melhor atende a esta proposta, alguns campos existentes tanto no estrutura lógica de dados quanto na zona legível por máquina precisarão ser modificados devido, por exemplo, a incompatibilidade com o tamanho do campo ou a necessidade de criação novos campos no padrão da ICAO (e.g. o campo onde serão armazenados os certificados de atributos).

Assim, acredita-se que é possível a utilização de forma segura de uma federação de identidade sem o risco de roubo de identidade ou comprometimento de dados, através do cartão de identidade. Além dos dados seguramente salvos, há também os dados impressos que possibilitam a leitura por agentes humanos ou por máquinas, tornando mais dinâmicas diversas atividades corriqueiras, como a verificação realizada na portaria de cinemas e teatros.

Com o cartão de identificação, que pode ser utilizado para qualquer fim, abre-se uma gama de possibilidade para a implementação de novos protocolos, como protocolos de autenticação e autorização, controle de presença em aulas, autenticação em cursos *online*, autenticação biométrica etc.

1.3 METODOLOGIA

No início do mestrado, definiu-se o tema que seria abordado e foi iniciada a revisão do estado da arte sobre federações de identidade: origem, funcionamento e federações existentes. Após o estudo de diversos artigos e dissertações sobre federações, foram identificados alguns problemas existentes no modelo de federação atual, destacando-se os problemas de segurança, privacidade e interoperabilidade. Neste processo, ficou definido que o método de pesquisa utilizado seria de natureza aplicada. Como visto em BARROS e Lehfeld (2007), a pesquisa aplicada tem como motivação a necessidade de produzir conhecimento para aplicação de seus resultados.

Posteriormente, foi realizado um estudo com o objetivo de encon-

trar formas de contornar problemas existentes no modelo de federação. Os trabalhos analisados concentram-se, principalmente, em artigos sobre federações e gerenciamento de identidade virtual e também o estudo de padrões de cartões de identificação, suas características, pontos positivos e negativos e aspectos de segurança do padrão. O padrão ICAO 9303, descrito no referencial teórico, foi o que melhor atendeu os requisitos do trabalho desenvolvido nesta dissertação.

Com o padrão escolhido, foi realizado um estudo da documentação e das características do padrão e um refinamento dos requisitos do cartão de identidade. Então, definiu-se a proposta da dissertação.

1.4 CONTRIBUIÇÕES

A primeira contribuição é o design de um cartão de identificação humano com um *QR Code*. A adição desse possibilita que os dados impressos no documento possam ser salvos no *QR Code* de forma assinada, garantindo a autenticidade e a integridade dos dados. Além disso, também é possível armazenar uma impressão digital de forma segura e assinada no *QR Code*, que pode ser usado como garantia de que o portador presente é o verdadeiro portador do cartão. Isso pode ser utilizado para autenticação biométrica com um baixo custo de emissão por parte da instituição emissora. Por essa proposta ser baseada no padrão dos passaportes, pode ser utilizado toda a infraestrutura já disponível para validação do mesmo, fazendo com que esse cartão seja uma extensão do passaporte e não um novo padrão, garantindo assim a interoperabilidade.

A segunda contribuição está relacionada com os cenários de uso do cartão de identificação considerando a infraestrutura disponível. Com esses cenários foi possível identificar formas de utilizar o cartão de identificação e quais equipamentos podem ser utilizados no processo de autenticação e autorização. A descrição desses cenários também possibilitou a validação do cartão de identificação através de cerimônias.

A terceira contribuição são as cerimônias de validação do cartão de identificação na forma de diagramas de sequência onde foram considerados os aspectos de segurança. No total foram descritos 11 cerimônias, levando em consideração as entidades participantes, seja essa humana ou não, e os poderes que cada entidade possui no âmbito da cerimônia. Com isso foi possível identificar alguns problemas de segurança presentes em cada situação e formas de resolver tais problemas.

Além das contribuições apresentadas nessa dissertação, houve

também uma publicação apresentando uma proposta de um cartão de identificação acadêmico baseada no padrão dos passaportes. A ideia inicial desta dissertação era a apresentação de um padrão de cartão de identificação voltada apenas para o meio acadêmico. Mais tarde essa ideia foi generalizada e transformada em um cartão de identificação humano. Essa ideia inicial foi publicada na conferência *International Conference on Availability, Reliability and Security (ARES)* com o título *A Proposal for an Unified Identity Card for Use in an Academic Federation Environment* (SASSO; MORAES; MARTINA, 2014).

1.5 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado da seguinte maneira. No Capítulo 2 é apresentado o estado da arte de Federações de Identidade e Cartões de Identidade, além de conceitos relacionados à Federações de Identidade e Gerenciamento de Identidade. No Capítulo 3 descrevemos o cartão de identidade federado proposto. No Capítulo 4 detalhamos alguns cenários onde o cartão de identificação pode ser utilizado e análises de segurança do cartão de identificação na forma de diagramas de sequência e finalizando no Capítulo 5 com as considerações finais e algumas sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

O objetivo deste capítulo é listar os casos de uso e exemplos de cartão de identificação, apresentando algumas Federações de Identidade e Cartões de Identificação existentes atualmente.

2.1 FEDERAÇÕES DE IDENTIDADE

As federações de identidade surgiram com o intuito de minimizar as demandas de credenciais para provedores de serviços. No lado do usuário, tem-se um menor número de contas utilizadas para acesso aos serviços, uma vez que o usuário poderá utilizar diversos serviços utilizando apenas uma credencial. Já no lado dos prestadores de serviços, simplifica-se o controle de acesso dos usuários, pois é possível receber credenciais de servidores especializados.

Os primeiros trabalhos envolvendo Federações foram propostos por volta de 2001 com a organização da *Liberty Alliance*. A *Liberty Alliance* foi uma organização formada para estabelecer normas e diretrizes no uso de federações (LIBERTY-ALLIANCE, 2003). Juntamente com o projeto *Liberty Alliance*, surgiu o projeto *Shibboleth* que também trabalha com gerenciamento de identidades federadas (SHIBBOLETH, 2014).

Em seguida, a *Microsoft Corpotarion* propôs o *Microsoft Passport*, que foi um percursor do modelo centralizado que está fundamentado no compartilhamento das identidades dos usuários entre provedores de serviços (MICROSOFT, 2003).

A partir do uso de federações de identidade no meio acadêmico, começaram a surgir parcerias entre instituições de ensino e pesquisa, surgindo assim federações acadêmicas de identidade. De acordo com Moreira et al. (2011), uma federação acadêmica de identidade envolve instituições de pesquisa e ensino. Uma federação permite que pessoas ligadas à essas instituições compartilhem informações e recursos e acessem serviços restritos, usando o vínculo institucional como um critério básico para essas operações. Wangham et al. (2010) cita que, em uma federação acadêmica, uma vez autenticado em sua instituição, é desejável que um usuário (do ponto de vista do mesmo) possa acessar qualquer serviço da federação sem novas autenticações, caracterizando o que é chamado de autenticação única (*Single Sign-On* - SSO). A Figura 1 mostra o funcionamento básico de uma federação acadêmica

(MOREIRA et al., 2011), onde representam-se dois acadêmicos de diferentes universidades (Universidade A e Universidade B) e diversos serviços oferecidos por cada universidade, como Correio Eletrônico, Administração e Sistema de Arquivos. Em um ambiente não-federado, para que um usuário da Universidade A possa utilizar um serviço da Universidade B, cada serviço deve manter informações sobre seus possíveis usuários, obrigando o utilizador a apresentar suas credenciais sempre que necessitar utilizar um serviço.

Em um ambiente federado as informações sobre os usuários são mantidos em um único local, normalmente a instituição em que o acadêmico possui seu vínculo principal, fazendo com que cada usuário necessite apenas de um registro (apenas um *login* e apenas uma senha) para desfrutar dos serviços. Com isso, se o usuário da Universidade B desejar utilizar um serviço da Universidade A, terá que apresentar suas credenciais apenas uma vez, pois as Universidades A e B fazem parte de uma federação e possuem um vínculo de confiança.

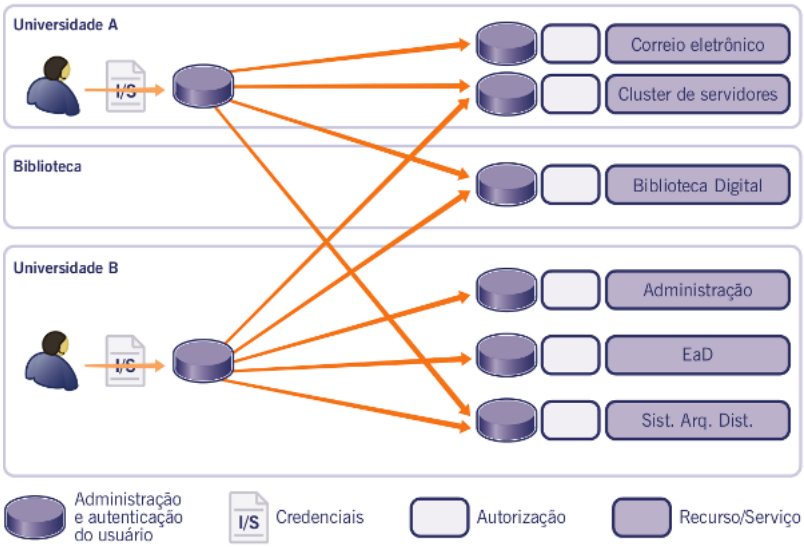

Figura 1 – Funcionamento de uma Federação

As federações de identidade tem como objetivo minimizar a manutenção de bases de dados e contas dos provedores de serviços e usuários. As informações sobre uma pessoa são mantidas em apenas um lugar e gerenciadas pela instituição de origem. Os Provedores de Ser-

viço confiam no gerenciador de identidade, fornecendo serviços para usuários das instituições e criando o princípio de identidade federada. Identidade Federada é uma ferramenta utilizada para autenticação de usuários de organizações parceiras, permitindo o compartilhamento de informações de identidade entre domínios seguros. Diversos países criaram suas federações acadêmicas, tais como:

- Estados Unidos (*InCommon*): A *InCommon* serve a educação e comunidades de pesquisa dos Estados Unidos da América, suportando um *framework* em comum para o gerenciamento confiável de compartilhamento de acesso a recursos *online*. Através da *InCommon*, usuários podem utilizar *single sign-on* nos Provedores de Identidade, além de existir uma proteção de privacidade, enquanto provedores de serviços controlam o acesso aos seus recursos protegidos (INCOMMON, 2014);

- Irlanda (*Edugate*): O *Edugate* provê um mecanismo de acesso simples que habilita o acesso a recursos *online*, suportando alianças, colaboração de pesquisa, consórcios e serviços compartilhados. Os usuários podem usar as credenciais emitidas pela sua instituição para o acesso aos serviços fornecidos pelo *Edugate*, com características de privacidade que colocam o usuário no controle de suas credenciais (EDUGATE, 2014);

- Itália (IDEM): O IDEM tem o objetivo de criar e manter um *framework* comum para a educação italiana e institutos de pesquisa para o gerenciamento de acesso a recursos *online*. Para atingir este objetivo o IDEM incentiva o desenvolvimento de uma comunidade baseada na confiança mútua. Deste modo, será fácil para os participantes tomar decisões corretas em matéria de controle de acesso, com base em informações fornecidas pelos próprios participantes (IDEM, 2014);

- Australia (*Australian Access Federation*): A *Australian Access Federation* (AAF) fornece os meios para permitir que uma instituição participante e/ou um Provedor de Serviço confie em uma informação que é recebida de uma outra instituição participante. Isso proporciona acesso a recursos e comunicação segura, pois remove a maior parte dos obstáculos para a colaboração e compartilhamento, tanto a nível de usuários institucionais e finais. Organizações também podem se beneficiar da AAF, pois a AAF permite que pesquisadores utilizem a sua instituição de origem

para utilizar um grande número de serviços e recursos (AUSTRALIAN ACCESS FEDERATION, 2014);

- Brasil (CAFe): A Comunidade Acadêmica Federada (CAFe) permite a cada usuário que possui uma conta, em sua instituição de origem, a autorização para todos os serviços fornecidos pela federação, eliminando a necessidade de múltiplas senhas e processos de registro. A relação de confiança entre instituições participantes da federação permite que usuários se autentiquem apenas em sua instituição de origem, que fornece garantias de autenticidade e credibilidade para as outras instituições participantes da federação (REDE NACIONAL DE ENSINO E PESQUISA, 2014).

Além destas federações acadêmicas, existentes em nível nacional, há também exemplos de federações em nível mundial, como é o caso do projeto *Eduroam*. O projeto *Eduroam* (*EDUcation ROAMing*) é um projeto europeu desenvolvido pela *Trans-European Research and Education Networking Association* (TERENA) (TERENA, 2014b) que visa proporcionar o acesso à Internet através de redes sem fio para a comunidade acadêmica. O Eduroam permite que estudantes, pesquisadores e funcionários de instituições parceiras tenham acesso à Internet quando visitarem outras instituições parceiras, fornecendo as credenciais da instituição de origem (WIERENGA; FLORIO, 2005) (TERENA, 2014a). Além disso, cada instituição tem que garantir a credibilidade das credenciais de seus usuários. Assim, o *Eduroam* utiliza uma relação de confiança entre as instituições através do conceito de federação (SAADE; CARRANO; SILVA, 2013).

2.2 CARTÕES DE IDENTIFICAÇÃO

Foram encontrados alguns trabalhos relacionados à criação de um cartão de identificação em nível mundial e a utilização do padrão dos passaportes na confecção de cartões de identificação.

No que tange aos trabalhos relacionados à criação de um cartão de identificação, o mais significativo, e talvez o único existente é o Cartão Internacional de Identificação Estudantil (do inglês *International Student Identity Card*, ISIC). O ISIC é reconhecida pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) como a única prova internacional de que uma pessoa é um estudante (ISIC, 2014b). O cartão ISIC é apoiado pela UNESCO desde 1965 (ISIC, 2014a) e é suportado pelo Conselho Europeu de Cultura e pela Comu-

nidade Andina das Nações. O cartão ISIC também é reconhecida por universidades, instituições acadêmicas, governos nacionais, instituições financeiras e ministérios da educação em todo o mundo (ISIC, 2014a). Apesar disso, o ISIC nada mais é do que um cartão com os dados impressos do estudante, onde o máximo de validação que é fornecido consiste em uma validação "cara-crachá". Não há nenhuma proteção eletrônica contra falsificação. Além disso, com o ISIC não existe a possibilidade de utilização de informações biométricas, para utilizar, por exemplo uma autenticação por impressão digital, uma vez que o cartão não armazena esse tipo de informação. A Figura 2 mostra um exemplo de cartão ISIC.

Figura 2 – Cartão Mundial do Estudante (ISIC, 2014a).

Com relação aos trabalhos relacionados à utilização do padrão dos passaportes para a criação de cartões de identificação, há trabalhos sendo feitos em diversos países. A Alemanha é um interessante exemplo, onde o *Personalausweis der Bundesrepublik Deutschland* (no português Bilhete de Identidade da República Federal da Alemanha) (FEDERAL MINISTRY OF INTERIOR, 2014b) foi instituído em 1º de Novembro de 2010, no formato de um *smartcard*, e possui algumas características de segurança interessantes, tais como:

- Impressão de segurança com uma estrutura de linhas multicoloridas;
- A guia alemã impressa como imagem tri-dimensional e latente;

- Impressão visível sobre luz ultra-violeta;
- Impressão tátil em alguns lugares;
- Um circuito integrado e seguro, incluindo o número do documento e o nome do portador;
- Uma imagem mutável na parte de trás, mostrando a validade do cartão de identidade ou o retrato do titular do cartão, dependendo do ângulo de visão;
- Apenas pessoas portando o cartão e que conhecem o PIN podem autorizar a transmissão de dados.

O cartão também possui a Função para Identificação Eletrônica (eID), que pode ser utilizada para identificar usuários na Internet de forma segura (FEDERAL MINISTRY OF INTERIOR, 2014a). O cartão também armazena uma fotografia e impressões digitais do portador, garantindo que o cartão de identidade realmente pertence a quem está portando, através de uma autenticação biométrica.

A Bélgica também possui um cartão de identidade que segue as recomendações da ICAO. Como visto em Cock, Wolf e Preneel (2006), o cartão belga possui três chaves RSA de tamanho 1024 bits. Dessas três chaves, uma é utilizada para autenticação do cidadão, a segunda é utilizada para o não-repúdio de assinaturas e a última para que o governo belga possa identificar o cartão. Os primeiros dois pares de chaves são acompanhados por certificados que são emitidos para o cidadão, utilizados para autenticação através do uso dos protocolos SSL/TLS, por exemplo.

Já na Itália, tem-se a *Carta d'Identità Elettronica*, conforme visto em (MINISTERO DELL'INTERNO, 2014a). O cartão de identidade eletrônico é um instrumento de identificação pessoal e autenticação para acesso aos serviços providos pela administração pública. As especificações técnicas do documento foram apresentados no Decreto Ministerial em 8 de Novembro de 2007 (MINISTERO DELL'INTERNO, 2014b). Os dados pessoais, número de residência, cidadania, código numérico da cidade do emissor, data de emissão e expiração, além de fotografia e assinatura de mão do portador são armazenados em um *microchip*.

Além da Alemanha, Bélgica e Itália, no Brasil também existem trabalhos relacionados à criação de um cartão de identidade baseada nas especificações do passaporte. O Registro de Identidade Civil (RIC) lançado oficialmente em 30 de Dezembro de 2010 tem um único objetivo: Que todo cidadão seja identificado por um único número. Com

isso, ao invés do cidadão ter diversos identificadores, um para cada situação, o número RIC será seu único identificador, substituindo documentos como o Cadastro de Pessoa Física (CPF), Registro Geral (RG), Título de Eleitor entre outros. As especificações técnicas foram apresentadas na Resolução nº 2 de 22 de novembro de 2011. Dentre as especificações apresentadas, destacam-se:

- Reconhecimento Óptico de Caracteres;
- Fotografia do Titular;
- Impressão o datiloscópica do anular direito do titular;
- Assinatura digitalizada do titular;
- Possuirá dois chips, um sem contato (para funcionar como um documento de viagem) e outro com contato (para questões de autenticação);
- Suporte a BAC.

Entretanto, os trabalhos com os novos cartões pararam RIC em 2011, sem notícias de continuidade (GLOBO, 2014).

2.3 GESTÃO DE IDENTIDADE

Como visto em Chadwick (2009), o gerenciamento de identidade consiste em um sistema integrado de políticas, processos de negócios e tecnologias que permite às organizações o tratamento e manipulações de identidade de seus usuários.

Conforme apresentado por Bhargav-Spantzel et al. (2007) um sistema de gerenciamento de identidades é caracterizado pelos seguintes elementos:

- Usuário: Pessoa ou equipamento vinculado a uma instituição e que utiliza os serviços fornecidos pelo Provedor de Serviços;
- Identidade: conjunto de atributos de um Usuário. Pode ser seu nome, endereço, filiação, data de nascimento, etc, ou algo que identifica um equipamento;
- Provedor de Identidade (*Identity Provider* - IdP): Os Provedores de Identidade são responsáveis por manter e gerenciar informações sobre as pessoas vinculadas a uma instituição (ROSSETO

et al., 2014). Essas informações podem ser o nome, CPF, sexo, data de nascimento, entre outros, além de vínculos do usuário em relação a instituição, como cargo ocupado, matrícula, data de admissão. Cada provedor de identidade deve estabelecer seu método de autenticação, além de garantir que cada Usuário tenha seu identificador único;

- Provedor de Serviços (*Service Provider* – SP): Os Provedores de Serviços oferecem serviços de acesso restrito, podendo requisitar privilégios de acesso baseados em informações adicionais sobre os usuários (como por exemplo, somente professores podem acessar um determinado serviço) (ROSSETO et al., 2014). Durante a implementação do serviço, são definidos os privilégios de acesso e as informações adicionais que serão solicitadas. É importante lembrar que manter informações sobre usuários é trabalho do IdP. O SP deve apenas solicitar tais informações ao IdP.

Quando há uma relação de confiança entre Provedores de Identidade e Provedores de Serviços de diferentes instituições, tem-se uma Federação de Identidade.

2.4 PROBLEMAS NO MODELO DE FEDERAÇÃO ATUAL

Foram encontrados, na literatura alguns, problemas existentes no modelo de federação atual, sendo que os principais são descritos a seguir.

2.4.1 Segurança

Roubo de identidade é uma séria preocupação em uma Federação de identidade (BHARGAV-SPANTZEL; SQUICCIARINI; BERTINO, 2005). Conforme visto em Bertino et al. (2010), o roubo de identidades digitais no ciberespaço é difícil de evitar, já que a informação digital pode ser copiada. Problemas relativos ao roubo de identidade podem afetar a todos os parceiros da federação. Um ataque também pode ser realizado roubando um token de segurança de um usuário autenticado, e assim, esse token pode ser usado para acessar recursos em um ambiente federado (HAN et al., 2010), o que pode ser comparado, por exemplo, com um ataque de sequestro de sessão, onde os *cookies* de sessão são roubados e utilizados com más intenções em um ambientes Web.

Consequentemente, mesmo sistemas com protocolos de autenticação mais seguros do que aqueles que utilizam nome de usuário e senha, estão expostos a ameaças de roubo de identidade (JENSEN, 2012) como os sistemas que usam autenticação de dois fatores onde, além do tradicional *login* e senha, é necessário que o usuário informe alguma outra informação, como um número aleatório gerado em um determinado intervalo de tempo em um dispositivo portátil (como um *smartphone*).

Jensen (2012) afirma que depois de um roubo de identidade bem sucedida dentro de uma federação, os atacantes podem comprometer os recursos de todos os prestadores de serviços federados, podendo levar à divulgação de dados sigilosos. Mais serviços podem ser acessados e mais dados podem ser comprometidos. Landau, Gong e Wilton (2009) identificam que a divulgação de dados pode ser um risco em níveis diferentes em uma federação: divulgação de dados da empresa, divulgação de metadados, sendo que este pode incluir a obtenção e mapeamento de atributos de usuários. Ahn e Lam (2005) também reconhecem a divulgação de dados como um desafio.

Técnicas para a proteção da confidencialidade e integridade são essenciais para prevenir o comprometimento de atributos de identidades ou modificação destes atributos. Mesmo que os atributos de identidade estejam protegidos através de mecanismos como a criptografia, Bertino et al. (2010) mostram que isso pode não ser o suficiente quando se trata de identidade. Muitas vezes os atributos de identidade devem ser divulgados a terceiros e validados quando é necessária a autenticação.

Ainda Bertino et al. (2010) destaca que não existem técnicas específicas previstas para proteção contra o mau uso de atributos de identidade armazenados nos Provedores de Identidade e Provedores de Serviços.

2.4.2 Privacidade

Conforme visto em Glasser e Vajihollahi (2008), as questões de segurança, privacidade e confiança no mundo digital, e mais particularmente na Internet, estão fortemente ligados a problemas de identidade. O que não é uma surpresa, considerando o ponto apresentado por Maler e Reed (2008), dizem que o principal objetivo do modelo atual de federação é compartilhar dados de identificação pessoal, e há uma grande preocupação no que diz respeito a privacidade.

Ahn e Lam (2005) apresentaram algumas preocupações de privacidade devido a grande troca de informações sensíveis de identidade

através de fronteiras organizacionais. Apesar de existirem políticas de privacidade e os usuários expressarem suas preferências de privacidade, há muita dificuldade para aplicá-las por meio da tecnologia. Ahn e Lam (2005) também acreditam que existe uma falta de apoio para fazer com que as preferências de usuários coincidam com as políticas de privacidade. E conforme apresentado por Squicciarini, Czeskis e Bhargav-Spantzel (SQUICCIARINI; CZESKIS; BHARGAV-SPANTZEL, 2008), desenvolver ferramentas que permitam aos usuários controlar o uso de suas informações de identidade não é trivial.

Conforme apresentado por Jensen (2012), uma solução para atenuar preocupações sobre privacidade é capacitar os usuários a controlar as suas identidades. De acordo com Bertino et al. (2010) as questões relacionadas com a forma como os utilizadores podem regular a divulgação e uso de suas informações de identidade não são devidamente abordados pelas especificações atuais de uma Federação de Identidade. Esse problema é também reconhecido por Shin, Lopes e Claycomb (2009). O fato de que os usuários em alguns casos, possuem um controle muito limitado sobre suas credenciais, e isso é considerado como um dos fatores que dificultam a utilização generalizada das tecnologias de Federações (BERTINO et al., 2010).

2.4.3 Interoperabilidade

Apesar dos esforços de normalização em federações, ainda existem desafios consideráveis com a interoperabilidade. Wolf et al. (2009) comentam que os protocolos de Federações trabalham em ambientes homogêneos. Entretanto, há situações em que os parceiros aderem a padrões diferentes, e isso aumenta a complexidade. Maler e Reed (2008) apontam para as opções de protocolo e variações de conformidade como aspectos que causam dificuldades. Além disso, podem haver várias necessidades relacionadas a atributos de identidade entre os parceiros dentro de uma federação. Speltens e Patterson (2007) apontam para acordos sobre semântica e uso dos atributos dentro de uma federação como o fator essencial para o sucesso de sistemas de federação. O processo de determinar quais são os atributos necessários e encontrar os atributos comuns e o esquema de dados para a cooperação interorganizacional pode ser um desafio (SPELTENS; PATTERSON, 2007) (BERTINO et al., 2010).

2.5 PASSAPORTE

Os passaportes são documentos de viagem que são emitidos pelo governo de uma nação. Um passaporte certifica a identidade e a nacionalidade de uma pessoa que está em uma viagem internacional (CANE; CONAGHAN, 2008). O termo *passport* vem de um documento que era requirido para alguém passar através de um portão (ou do inglês *porte*) em uma cidade na idade medieval (DONALD, 1867).

Conforme visto em Casciani (2008), a referência mais antiga ao documento aparece durante o reinado de Henry V, datado em 1414. Esse documento geralmente continha uma lista de cidades onde o portador era autorizado a entrar. Esse passaporte manteve o formato rudimentar por um longo tempo, e na falta de um retrato do portador, alguns documentos continham uma descrição física do portador.

O primeiro passaporte a conter um retrato do portador apareceu no início do século XX. Após as duas primeiras guerras, as Nações Unidas, juntamente com a ICAO publicaram um guia para padronizar o formato dos passaportes. Essas especificações foram mais tarde publicadas na documentação 9303 da ICAO.

2.5.1 Documentação ICAO 9303

O padrão ICAO 9303 é uma série de documentos criados pela ICAO, que tem como objetivo descrever as especificações dos Documentos de Viagem Legíveis por Máquinas (MRTD).

Como descrito no website da ICAO, o passaporte ICAO foi estabelecido em 1968, no ICAO *Panel on Passport Cards*. Nesse painel, foram preparadas as recomendações para padronizar os documentos de viagem, acelerando assim a liberação de passageiros no controle de passaportes em aeroportos. Mais tarde, as especificações foram publicadas na primeira edição da documentação 9303 e hoje é usado como um guia em todo o mundo para emissão de documentos de viagem (ICAO, 2014).

A documentação ICAO é dividida em 3 partes. A parte 1, que possui dois volumes, apresenta as especificações para os Passaportes Legíveis por Máquinas, especificando como salvar os dados em OCR, e como utilizar Identificação Biométrica. A parte 2 especifica os Vistos Legíveis por Máquinas. E a parte 3, que também possui dois volumes, define como devem ser os Documentos de Viagens Oficiais Legíveis por Máquinas. Na Figura 3 é mostrada o formato geral de um passaporte.

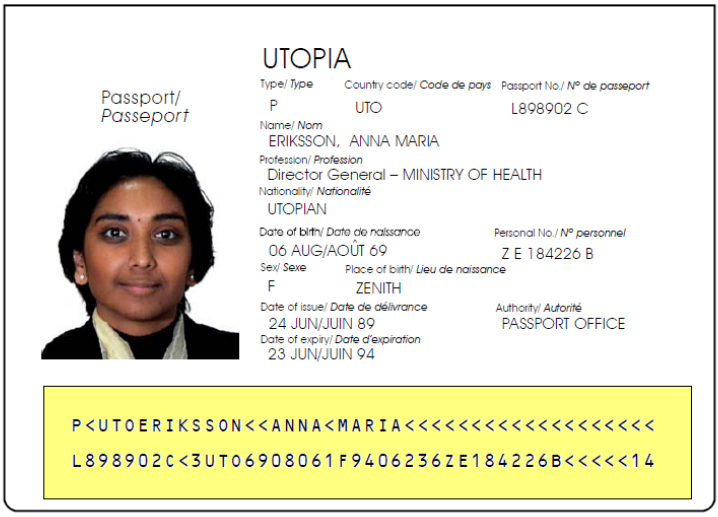

Figura 3 – Formato geral de um passaporte

2.5.1.1 Zona de Inspeção Visual

Conforme descrito na documentação da ICAO (ICAO, 2008a), a Zona de Inspeção Visual (*Visual Inspection Zone*, VIZ) consiste em zonas que contêm campos de dados obrigatórios e opcionais para acomodar as diferentes necessidades dos estados emissores. Em outras palavras, a VIZ pode ser descrita como a seção onde dados como nome, data de nascimento e número do passaporte estarão impressos no passaporte, utilizados para a inspeção visual por humanos.

2.5.1.2 Zona Legível Por Máquina

Os documentos que seguem o padrão 9303 utilizam uma Zona Legível Por Máquina (do inglês *Machine readable zone*, MRZ) para facilitar a inspeção de documentos. O MRZ fornece elementos de dados formatados para serem legíveis por máquinas que seguem o padrão MRTD. Estes dados devem ser lidos tanto por máquinas quanto por humanos. Como solução para esses requerimentos, um OCR foi espe-

cificado na documentação 9303 como uma forma de salvar e coletar dados do MRZ. A Figura 4 mostra o formato do MRZ nos passaportes, conforme apresentado na documentação (ICAO, 2008a).

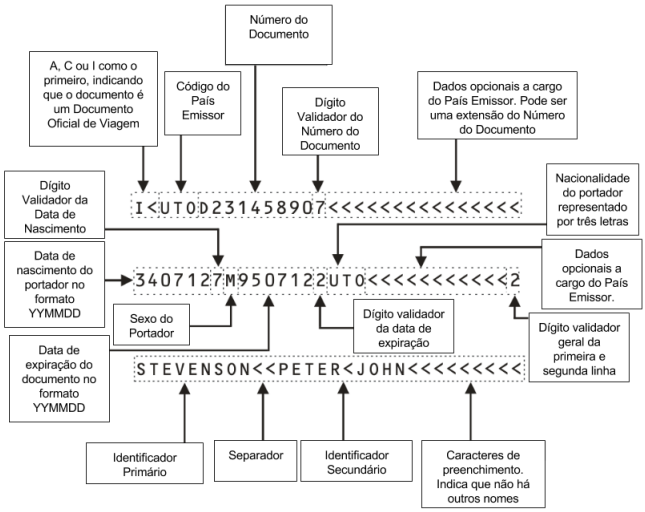

Figura 4 – Zona Legível por Máquina no Passporte.

No MRZ, estão contidas informações chave sobre o portador do documento. Na primeira linha, estão os dados que indicam qual o tipo do documento, o estado emissor e o número do documento. Na segunda linha, estão os dados de usuário, como data de nascimento, sexo, nacionalidade, além da data de expiração do documento. Na terceira linha, está o nome do portador do documento.

2.5.1.3 Estrutura Lógica de Dados

Um documento MRTD também possui um Circuito Integrado sem contato (CI). A *Logical Data Structure* (LDS) descreve como os dados são escritos no CI e como são formatados, garantindo a interoperabilidade global para leitura por máquinas (ICAO, 2008b).

O LDS possui alguns dados obrigatórios e outros opcionais. Esses dados estão agrupados por Data Groups (DG), dependendo de onde eles

são gravados. A Figura 5 mostra a estrutura lógica de um passaporte, conforme apresentado na documentação (ICAO, 2008b) .

Detalhes Salvos no MRZ
Grupo de Dados 1
Tipo do Documento
Estado Emissor
Nome do Portador
Número do Documento
Dígito Validador do Número Documento
Nacionalidade
Dígito Validador da Data de Nascimento
Sexo
Data de Validade
Dígito Validador da Data de Validade
Dados Opcionais
Dígito Validador dos Dados Opcionais
Dígito Validador Geral

Codificação das Características de Identificação		
Para Intercâmbio	Grupo de Dados 2	Codificação da Face
Características Adicionais	Grupo de Dados 3	Codificação das Digitais
	Grupo de Dados 4	Codificação da Iris
Características de Identificação Impressas		
Grupo de Dados 5	Retrato Impresso	
Grupo de Dados 6	Reservado para Uso Futuro	
Grupo de Dados 7	Assinatura Impressa	
Codificação das Características de Segurança		
Grupo de Dados 8	Características de Dados	
Grupo de Dados 9	Características de Estrutura	
Grupo de Dados 10	Características de Substância	
Grupo de Dados 11	Detalhes Pessoais Adicionais	
Grupo de Dados 12	Detalhes Adicionais do Documento	
Grupo de Dados 13	Detalhes Opcionais	
Grupo de Dados 14	Opções de Segurança para Biometria Secundaria	
Grupo de Dados 15	Informações da Chave Publica para Autenticação Ativa	
Grupo de Dados 16	Pessoas para Notificar	
Versões Futuras do LDS		
Grupo de Dados 17	Apuramento Automatizado de Fronteira	
Grupo de Dados 18	Visto Eletrônico	
Grupo de Dados 19	Registros de Viagem	

Figura 5 – Estrutura Lógica de Dados no Passaporte.

Dentre todos estes dados, os obrigatórios são os que pertencem aos Grupo de Dados 1 e Grupo de Dados 2, que possuem os dados presentes na Zona de Legível por Máquina e Dados Biométricos respectivamente. As informações biométricas, tais como dados para o reconhecimento facial, impressão digital e íris são armazenados nos grupos 2, 3 e 4, respectivamente.

Em adição a estes grupos, o CI também contém outros grupos onde importantes informações são armazenadas, como:

- Grupo de Dados 7: Utilizado para armazenar assinatura de mão do portador;
- Grupo de Dados 11 (Detalhes pessoais adicionais): Informações

pessoais como endereço, ocupação, nome dos pais e número de telefone;

- Grupo de Dados 12 (Detalhes adicionais do documento): Informações sobre o emissor do passaporte;
- Grupo de Dados 16 (Pessoas para notificação): Informações sobre pessoas que devem ser notificadas em caso de emergências.

O LDS também contém um cabeçalho e um *Data Group Presence Map*, que está armazenado em um arquivo EF.COM. Esse cabeçalho contém as informações que permitem localizar e decodificar os grupos de dados. A confirmação de autenticidade e integridade dos dados armazenados é feita pelo *Security Object*. Cada grupo de dados é representado neste objeto, que é armazenado em um arquivo EF.SOD. Esses dois arquivos são obrigatórios (ICAO, 2008a).

2.5.1.4 Mecanismos de proteção

O Circuito Integrado não possui qualquer mecanismo de controle de acesso, o que leva a possíveis ataques:

- Os dados armazenados no Circuito Integrado sem contato podem ser eletronicamente lidos por um atacante apenas por aproximação e sem que o atacante tenha o documento em mãos, possibilitando uma clonagem;
- A comunicação não criptografada entre o Circuito Integrado sem contato e a leitora pode ser espionada em uma distância de alguns metros.

Como uma forma de proteger os dados do circuito contra esses ataques, a ICAO sugere e descreve na Documentação 9303 alguns mecanismos de segurança. Apresenta-se a seguir cada um deles.

2.5.1.4.1 Controle Básico de Acesso

Para evitar a leitura sem autorização dos dados é recomendado o uso de um Controle Básico de Acesso (do inglês *Basic Acess Control* (BAC)).

O mecanismo BAC permite acesso ao Circuito Integrado apenas se o solicitante provar que está autorizado a acessar o LDS. Isso é

fornecido por um protocolo desafio-resposta, onde o solicitante prova que tem o acesso ao *Document Basic Access Key*. Essas chaves podem ser fornecidas por um leitor MRZ ou manualmente. Com o intuito de aumentar a segurança, após a autenticação, o Circuito Integrado deve criptografar/cifrar o canal de comunicação com o solicitante (ICAO, 2008b). A seguir, descreve-se como funciona o desafio-resposta:

1. O solicitante fornece algumas informações presentes no MRZ, que é a concatenação do Número do Documento, Data de Nascimento e Data de Validade. Esses dados estão impressos no documento e podem ser coletados usando um leitor OCR ou manualmente;

2. Tanto o Circuito Integrado quanto o solicitante geram uma chave de sessão;

3. Um processo de autenticação é realizado, e posteriormente, os dados são enviados por um canal seguro.

O desafio-resposta deve ser cifrado utilizando duas chaves 3DES no modo CBC. A autenticação do protocolo deve ser calculada usando *Message Authentication Codes* (MAC) (ICAO, 2015).

2.5.1.4.2 Autenticação Passiva

O LDS tem um *Document Security Object* (SOD) que é assinado pelo emissor e contém um *hash* cifrado com uma chave privada do conteúdo do LDS. Qualquer um com a chave pública do assinador do documento pode verificar a integridade do SOD, e consequentemente a integridade do LDS. Esse processo é chamado Autenticação Passiva (AP) e é utilizado para verificar se os dados no chip de um documento de identificação eletrônico são autênticos e não forjados (FEDERAL OFFICE FOR INFORMATION SECURITY, 2015). Como o circuito integrado possui um arquivo assinado contendo *hashs* dos dados armazenados, se ocorrer qualquer modificação em um desses dados do circuito, essa alteração poderá ser detectada quando o valor *hash* do dado alterado não for equivalente ao valor *hash* presente no arquivo SOD. Para esse esquema funcionar, o mecanismo usa uma infraestrutura de chaves públicas dedicada.

Esse processo prova a autoria e a integridade dos dados, mas isso não previne a substituição do chip ou a cópia do conteúdo. Uma forma de prevenir a substituição do chip é usando Autenticação Ativa (AA) .

2.5.1.4.3 Autenticação Ativa

Conforme visto em Saeed, Masood e Kausar (2009), a Autenticação Ativa é usada para evitar a clonagem de chips, sendo utilizado um protocolo desafio-resposta, em que o chip do passaporte comprova à leitora a posse da chave privada. A chave é armazenada em um espaço de memória inacessível no chip. A chave pública correspondente é armazenada no Grupo de Dados 15 do chip que é acessível à leitora (SAEED; MASOOD; KAUSAR, 2009).

2.5.1.4.4 Controle de Acesso Estendido

Conforme descrito por Mostowski e Poll (2010), o Controle de Acesso Estendido consiste em dois protocolos:

- Autenticação do Chip: Um protocolo para o terminal autenticar o chip. A autenticação do chip é baseada em um acordo de chaves secretas e estabelece novas chaves de sessão.
- Autenticação do Terminal: um protocolo para o chip autenticar o terminal, e aumentar os direitos de acesso. A autenticação do terminal é feita com uma verificação ativa de certificados e uma requisição de autenticação enviada ao passaporte pelo sistema de inspeção.

Ambos protocolos dependem de uma Infraestrutura de Chaves Públicas, onde cada país emite certificados para seus passaportes (para a autenticação do Chip) e certificados para outros países para que estes possam ler dados mais sensíveis do passaporte (para Autenticação do Terminal).

Ainda citando Mostowski e Poll (2010), o Controle de Acesso Estendido protege o acesso as impressões digitais e iris armazenadas no passaporte.

2.6 CONSIDERAÇÕES SOBRE CAPÍTULO

As Federações de Identidade são uma realidade, onde um usuário não precisa memorizar diversas contas para acessar os diversos serviços providos de diferentes instituições e outros parceiros, constituindo-se também em uma vantagem para as instituições, pois, não é preciso

manter e gerenciar diversas bases de dados com informações de autenticação de usuários. No entanto, conforme descrito neste capítulo, as federações de identidade de um modo geral apresentam alguns problemas de segurança, e.g. roubo de identidade, comprometimento e privacidade de dados e interoperabilidade que precisam de alguma forma ser contornados. A ICAO através da documentação 9303 apresenta um padrão que pode ser utilizado para resolver esses problemas.

No próximo capítulo, apresentar-se-á em detalhes a proposta de cartão de identificação, com uma explicação das alterações realizadas e também de cada componente.

3 PROPOSTA

A proposta apresentada nesta dissertação funde a ideia de documentos legíveis por máquinas com federações de identide. Para resolver alguns dos problemas presentes em ambientes federados, como mencionado anteriormente, planeja-se adaptar o padrão da ICAO para atender as necessidades de ambientes federados, onde haverá uma identidade para utilização em tal ambiente. Neste capítulo detalha-se a proposta deste cartão de identificação.

3.1 ZONA LEGÍVEL POR MÁQUINA

Como já foi descrito, o passaporte utiliza OCR, permitindo que o documento possa ser legível tanto por pessoas quanto por máquinas. Comparado com o MRZ original, no MRZ do cartão foi feita uma alteração na primeira linha. Originalmente, a primeira linha continha dois dígitos para o tipo de documento, três para o país emissor, nove para o Número do Documento, um para o dígito de validação e quinze dígitos de Informações Opcionais. A proposta para o MRZ no cartão de identidade é manter o número de dígitos para o Tipo de Documento e Estado Emissor. Porém, definiu-se dois tipos de documento: *Id Student* (IS) ou *Id Academic* (IA). Isso permitirá que o documento possa ser avaliado por humanos para identificar acadêmicos em suas taxas de descontos, como descontos de meia entrada em cinema ou teatros. Nas posições de Estado Emissor, teremos o País da instituição que emitiu o cartão. Isso permitirá que uma leitora por exemplo após ler e extrair os dados do cartão de identificação, possa de alguma forma fazer uma verificação se os dados do documento são válidos ou não, entrando em contato com a Infraestrutura de Chaves Públicas da Federação ou país no qual o cartão foi emitida.

O Número do Documento será de tamanho variável, além de ter o dígito de validação. Nos dados opcionais na primeira linha, haverá a sigla da instituição, que estará separado do Número do Documento pelo carácter $<$. A figura 6 mostra a proposta para o MRZ em um cartão acadêmico.

Resumidamente, propõe-se:

Primeira linha

Posição 1 a 2: Os caracteres devem ser IS (Id Student) ou IA (Id Academic) para indicar que este é um documento de identificação.

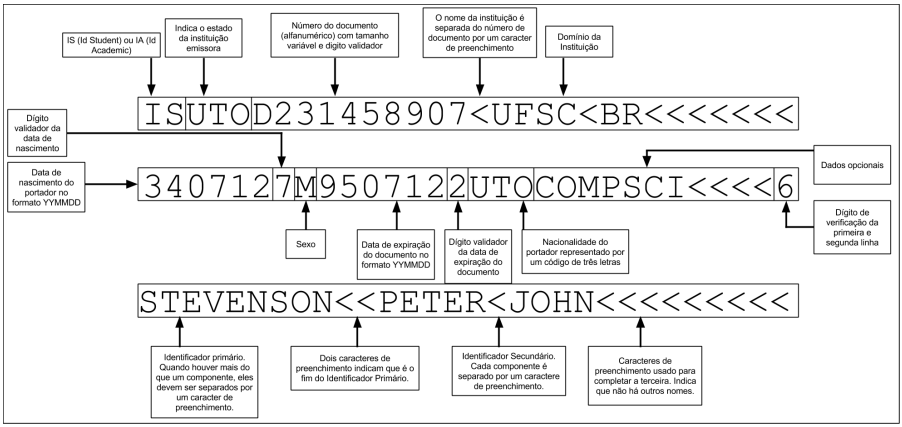

Figura 6 – Zona Legível por Máquina no Cartão de Identificação

Posição 3 a 5: O código de três letras para indicar o país da instituição emissora, conforme definido na ISO 3166-1 alfa-3 (ISO, 2000a).
Posição 6 a 30: Número de Identificação de 9 dígitados e o dígito validador do mesmo. Após o carácter separador (<), pode-se colocar o domínio da Instituição de origem (por exemplo, ufsc.br), substituindo o ponto por mais um carácter separador (<).
Segunda linha:
Posição 1 a 6: Data de nascimento do titular no formato YYMMDD.
Posição 7: Dígito validador da data de nascimento.
Posição 8: Sexo do titular.
Posição 9 a 14: Data de expiração do documento no formato YYMMDD.
Posição 15: Dígito validador da data de vencimento.
Posição 16 a 18: Nacionalidade do portador representado por um código de três letras.
Posição 18 a 29: Dados opcionais, a critério da instituição.
Posição 30: No geral, é o dígito validador para a primeira e segunda linhas.
Terceira linha:
Posição 1 a 30: Nome do Portador. O nome consiste em identificadores primários e secundários, que devem ser separados por dois carácteres <. O caráter < deve separar os componentes dentro dos identificadores primários ou secundários. Quando o nome do titular do documento tem apenas um nome, deve ser colocado em primeiro lugar na posição para identificadores primários e o resto da linha deve ser preenchido com <.

3.2 ZONA DE INSPEÇÃO VISUAL

Com exceção dos dígitos validadores, todos os outros dados contidos no MRZ são impressos no documento, permitindo a leitura visual. Além do OCR, o cartão acadêmico também possuirá um *QR Code*, contendo todos os dados do MRZ. Isto permitirá que universidades possam desenvolver seus próprios aplicativos para ler o código. Há também a possibilidade de salvar dados do MRZ de forma assinada no *QR Code*, o que garante a autenticidade dos dados impressos. Assim, as universidades tem a opção de evitar gastos com compras de leitoras específicas para passaportes, que possuem um alto custo, além de serem complicadas de gerenciar. Há também a possibilidade de ser usado um smartphone ou tablet com Near Field Communication (NFC) e câmera para leitura dos dados do cartão. As figuras 7 e 8 mostram como será a Zona de Inspeção Visual de um cartão de identificação.

Figura 7 – Anverso de um cartão de identificação

3.2.1 QR Code

Um *QR Code* (abreviado de *Quick Response Code*, Código de Resposta Rápida) é a marca registrada de um tipo de código de barras em forma de matriz desenhado para uso na indústria automotiva japonesa. Um código de barras é um rótulo legível por máquina que contém informações sobre o item no qual está anexado. Um *QR code* usa quatro modos de codificação padronizado para armazenar dados: numérico, alfanumérico, *byte*/binário e caracteres da língua japonesa, o kanji. As especificações do *QR code* são descritas na ISO 18004 (ISO, 2000b).

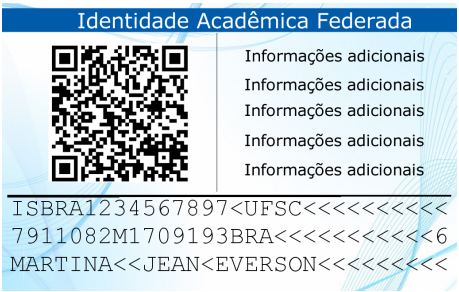

Figura 8 – Verso de um cartão de identificação

3.2.1.1 Características

Conforme apresentado na ISO 18004 (ISO, 2000b), um *QR Code* possui diversas características. Em um *QR Code*, é possível codificar dados numéricos e alfanuméricos, como número de 0 a 9, letras maiúsculas de A a Z, entre outros caracteres, como o Kanji. Também é possível codificar dados de 8 bits.

Os dados são representados por módulos negros e claros, onde os módulos negros representam o binário 1 e os módulos claros representam o binário 0. Um *QR code* pode ser impresso em diversos tamanhos de acordo com o número de módulos, variando de tamanhos de 21 x 21 módulos até 177 x 177 módulos.

O *QR code* também possui 4 níveis de correção de erros, permitindo a recuperação de um percentual de dados de acordo com o nível. Descrevemos brevemente cada um a seguir:

- Nível L (Baixo): 7% de dados podem ser recuperados;
- Nível M (Médio): 15% de dados podem ser recuperados;
- Nível Q (Quarto): 25% de dados podem ser recuperados;
- Nível H (Alto): 30% de dados podem ser recuperados;

3.2.1.2 Estrutura

Conforme descrito na ISO 18004 (ISO, 2000b), um *QR code* deve ser construído com módulos de formato quadrado distribuídos em uma matriz também de formato quadrado. Esta matriz deve possuir regiões de codificação e funções de reconhecimento de padrões. O *QR Code*

deve ser cercado nos quatro lados por uma margem em branco. A Figura 9 detalha a estrutura (ISO, 2000b).

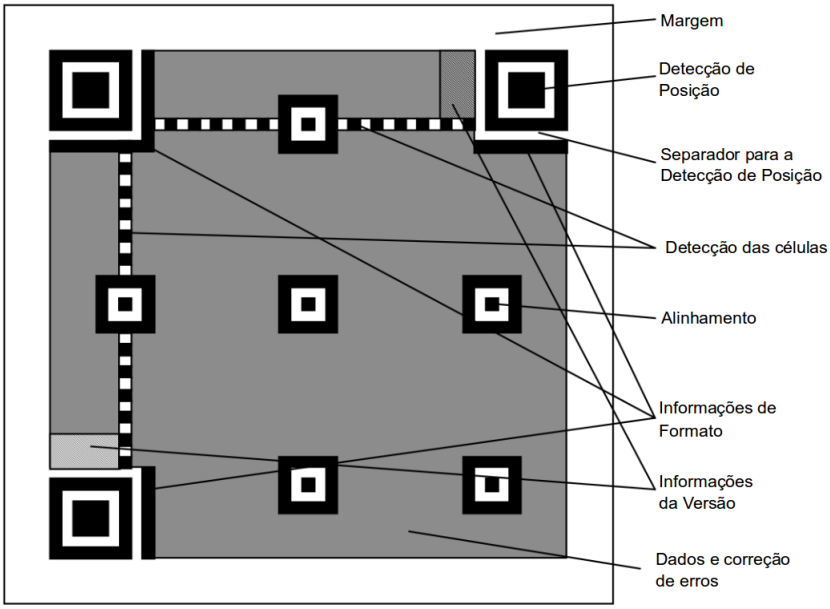

Figura 9 – Estrutura do *QR code*.

A Detecção de Posição permite uma rápida localização de um possível *QR code* no campo de visão. A identificação dos três padrões mostrado na Figura 9 definem a localização e orientação do símbolo no campo de visão. O separador organiza cada padrão de Detecção de Posição da região de codificação.

A Detecção de Célula consiste em uma linha e uma coluna composta por módulos que alternam na cor branca e escura, começando e terminando com módulos escuros, permitindo a localização de cada módulo na área codificada.

A região de codificação contém os símbolos representando dados, os códigos de correção de erro, informações de versão e informação de formato. E por fim a margem em branco tem como objetivo destacar o *QR code* de qualquer superfície no qual este está sendo aplicado.

3.3 ESTRUTURA LÓGICA DE DADOS

A Estrutura Lógica de Dados prevê campos que podem ser usados para autenticação biométrica, como os campos Codificação da Face, Codificação da Digital e Codificação da Iris no Grupos de Dados 2, 3 e 4. Em adição aos campos já presentes na estrutura, sugere-se a inclusão de um Campo de Autorização, onde podem ser armazenados os certificados de atributos para o controle de acesso, entre outras informações. A Figura 10 mostra como será a Estrutura Lógica de Dados do cartão de identificação.

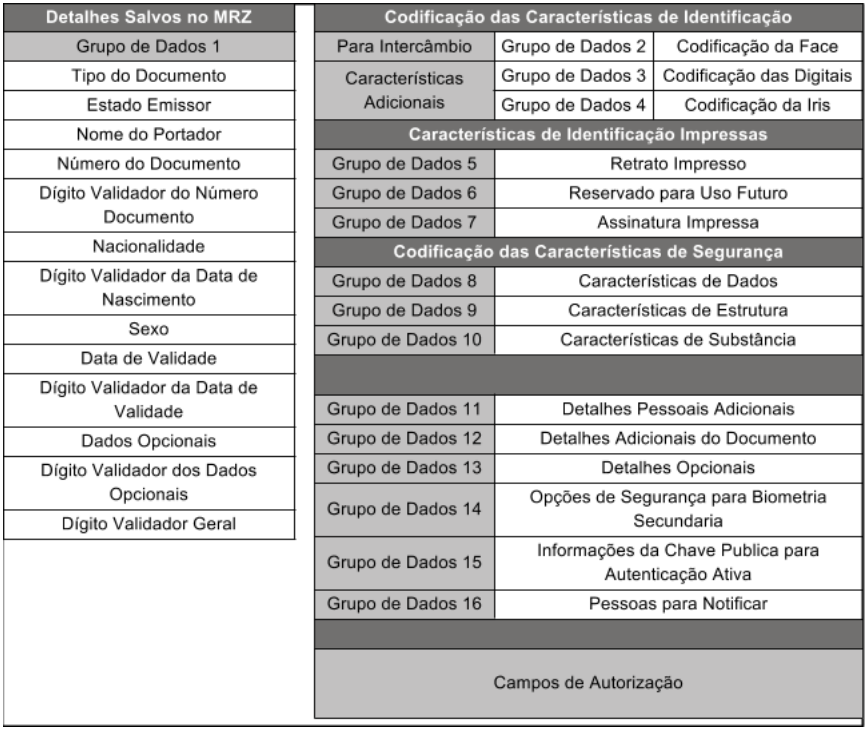

Figura 10 – Estrutura Lógica de Dados do cartão de identificação.

3.3.1 Uso de Certificados de Atributos.

Um certificado de atributo (ou certificado de autorização) é um documento eletrônico que contém um conjunto de atributos que se relacionam ao titular. Seu formato e sintaxe são definidos pelo padrão X.509, o mesmo padrão usado para certificados digitais (ITU, 2000). O certificado de atributo não tem chave pública. É digitalmente assinado por uma autoridade confiável (chamado de Entidade Emissora de Certificados de Atributos). Este certificado pode ser usado sozinho ou em conjunto com um certificado digital. Assim, os atributos no certificado podem ser alterados ou mesmo revogados, sem envolver a revogação de certificados digitais. É possível armazenar os Certificados de Atributos nos Campos de Autorização do cartão de identificação. Os Certificados de Atributos podem ser usados para muitas finalidades diferentes, entre elas:

- Melhor caracterização do portador;
- Informações de autorização;
- Identificação de grau, departamento, ano de início e final do curso;
- Delegação de autoridade.

A proposta é que cada instituição assume a responsabilidade pela emissão dos certificados, que pode ser escrito no cartão de identificação no momento da criação e de forma segura. Na prática, o portador com o presente cartão iria provar a sua identidade e com o certificado de atributo, garantir o seu vínculo a uma instituição e quaisquer outros dados opcionais não padronizados pela proposta.

3.4 IMPLANTAÇÃO INCREMENTAL

Seguindo essa proposta, é possível que entidades com recursos financeiros limitados também possam aderir ao padrão. Seguindo a proposta historicamente estabelecida pela ICAO, as entidades terão cinco opções para a emissão do cartão proposto, conforme descrito nas seções seguintes.

3.4.1 Tipo 1: Apenas a Zona de Inspeção Visual

O cartão do Tipo 1 pode ser emitido por instituições que possuem recursos financeiros limitados ou em casos em que não há a necessidade

de uso de leitura mecânica ou biometria. Basicamente, como pode-se observar na Figura 7 apresentada anteriormente, há um cartão onde são impressos dados apenas no anverso, sem a existência de uma Zona Legível por Máquina e uma Estrutura Lógica de Dados. Esse tipo de documento apenas poderá ser avaliada por agentes humanos.

3.4.2 Tipo 2: Zona de Inspeção Visual com Zona Legível por Máquina

Basicamente o Tipo 2 possui, a Zona de Inspeção Visual descrita no Tipo 1, e uma Zona Legível por Máquina. Conforme mostrado anteriormente na Figura 8, impresso no verso há um *QR Code* e uma banda com Reconhecimento Ótico de Caracteres.

Este tipo pode ser emitido por instituições que além de ser legível para agentes humanos, necessitem de validações que podem ser impostas por meio eletrônico.

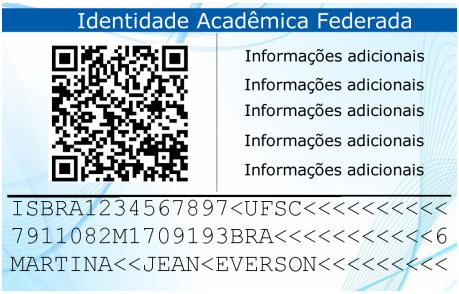

Figura 11 – Verso de um Cartão Tipo 2.

3.4.3 Tipo 4: Total funcionalidade

O cartão Tipo 4 possui todas as características presentes no Tipo 1 e Tipo 2 com a adição de um Circuito Integrado com Contatos. Como já citado anteriormente, o Circuito armazena diversos dados de forma segura, onde apenas entidades autorizadas pelo emissor podem ter acesso a alguns Grupos de Dados, como dados biométricos (digitais e iris) para autenticação biométrica e outros dados do portador. A Figura 12 mostra o anverso de um cartão de identificação Tipo 4, onde há a adição do Circuito Integrado.

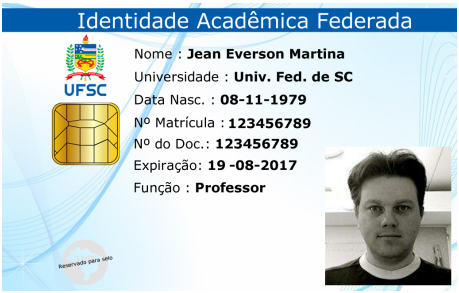

Figura 12 – Verso de um cartão Tipo 4.

3.4.4 Tipo 5: Total funcionalidade com circuito sem contato

De forma resumida, o Tipo 5 tem as mesmas funcionalidades do Tipo 4, entretanto o Circuito Integrado nesse caso é sem contato. Isso permite a instituição criar seus próprios sistemas onde o portador apenas aproxima o cartão da leitora sem contato, tornando o processo de validação muito mais rápido. Obviamente, um cartão do Tipo 5 custará mais caro que os outros.

3.4.5 Tipo 3: Zona de Inspeção Visual com Zona Legível por Máquina e biometria segura

O Tipo 3 pode ser emitido por instituições que necessitem de uma autenticação biométrica mas que não tem recursos para um cartão do Tipo 4 ou Tipo 5, ou que não precisem de todas funcionalidades oferecidas por tais. No verso deste tipo de documento, além do MRZ, há um código de barras 2D onde pode ser armazenado o *template* de uma digital de forma segura e assinada. Este modelo foi sugerido por Távora, Torres e Fustinoni (2015). Nesse modelo, apenas entidades autorizadas podem decifrar a biometria salva no código de barras 2D. A Figura 13 mostra o verso de um Cartão de Identificação do Tipo 3.

3.5 CONFECÇÃO DO CARTÃO

Foi realizada a confecção de um protótipo do cartão de identificação apresentado nesta dissertação. Isso ocorreu no Programa de Gestão

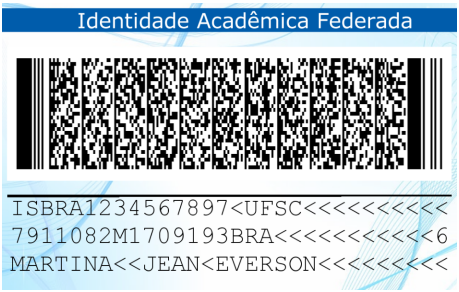

Figura 13 – Verso de um Cartão Tipo 3.

de Identidade no ano de 2014 da Rede Nacional de Ensino e Pesquisa. O cartão utilizado possui um circuito integrado com contatos e sem contatos. Foram armazenados alguns dados no cartão e impresso os dados no mesmo. Um relatório apresentando todo o desenvolvimento do projeto pode ser encontrado na página do Comitê Técnico de Gestão de Identidade (RNP, 2014).

3.6 CONSIDERAÇÕES SOBRE CAPÍTULO

Com essa proposta espera-se contornar os problemas existentes atualmente em federações. Com cartões de identificação sendo utilizadas em federações seguindo um mesmo padrão, resolve-se o problema de interoperabilidade apresentado anteriormente. Além disso, com as credenciais armazenadas de modo seguro no cartão evita-se problemas como roubo de identidade, uma vez que esses dados não precisam ficar vagando diversas vezes pela *Internet*. E com os dados impressos no cartão, elimina-se a necessidade de comunicação *online* para atividades mais simples. Com o cartão no padrão ICAO, abre-se também a possibilidade de autenticação biométrica, sendo que os dados mais sensíveis podem ser salvos no cartão de forma segura.

4 AVALIAÇÃO E USO DO CARTÃO DE IDENTIFICAÇÃO

4.1 APLICAÇÕES DO CARTÃO DE IDENTIFICAÇÃO

O cartão pode ser utilizado em diversas atividades. Nas Seções seguintes detalhar-se-á alguns cenários de uso.

4.1.1 Controle de presença

As instituições de ensino podem utilizar as funcionalidades do cartão como uma forma de automatizar o controle de presença em sala de aula. Uma vez que não há a necessidade real de um atendente para realizar o processo, este poderá ser mais agilizado.

A universidade pode usar cartões do Tipo 3 em conjunto com leitoras *QR Code* e leitoras biométricas para garantir que somente o verdadeiro Portador possa comprovar sua presença em sala de aula. Basicamente o Portador do documento apresenta o cartão com o *QR Code* ao leitor onde será verificado a assinatura dos dados armazenados no código. Após, será solicitado que o usuário apresente sua digital para que o sistema verifique se é o verdadeiro Portador que está apresentando o cartão, fazendo com que o sistema confirme a presença em sala do aluno. Este caso de uso se enquadra no Procedimento 11 na Seção 4.13.

Para documentos do Tipo 4, ao invés de um leitor *QR Code*, usa-se um leitores de *Smart Cards* em conjunto com Leitoras Biométricas. Nesse caso, o Portador insere seu cartão na leitora e informa os dados necessários para sistema ler os dados salvos no cartão e realizar uma validação da assinatura digital. Após, será solicitado que o usuário apresente sua digital para que o sistema verifique se é o verdadeiro Portador que está apresentando o cartão, fazendo com que o sistema confirme a presença em sala do aluno. Este caso de uso se enquadra no Procedimento 9 na Seção 4.11.

Já para um cartão do Tipo 5, pode-se usar uma leitora Sem Contato, uma vez que este documento possui um circuito integrado sem contato. Assim como na cartão do Tipo 4, é feita uma validação de assinatura dos dados armazenados no cartão e uma verificação biométrica para a comprovação de que é o verdadeiro Portador que está presente. Este caso de uso se enquadra no Procedimento 9 na Seção 4.11.

4.1.2 Autenticação em Cursos Online

Como visto em Haggard (2013), cursos *online* tem rapidamente ganho popularidade, expansão e evolução. Alguns cursos *online* fornecem certificados de conclusão para as atividades feitas, que podem tanto melhorar o currículo de quem o está fazendo quanto ser utilizado para validação de disciplinas em aulas presenciais. Entretanto, atualmente, não há uma forma de garantir que o aluno que está inscrito no curso é a pessoa que está fazendo as tarefas e sendo avaliada. É possível resolver isso com um agente humano observando o usuário e suas ações. Entretanto, para isso, é necessário uma pessoa estar disponível para tal tarefa.

O sistema pode usufruir do que o cartão de identificação oferece (mais especificamente o Tipo 4 e Tipo 5) para automatizar este processo através de uma autenticação contínua, onde o sistema necessita de métodos para autenticar continuamente o usuário baseando-se em traços biométricos (NIINUMA; JAIN, 2010). Esta situação se encaixa na Situação 8 na Seção 4.10, onde um usuário que deseja realizar um curso *online* precisará de um leitor *Smart Card*, uma câmera e um leitor biométrico.

Com isso em mãos, basicamente o aluno insere o cartão no leitor *Smart Card*, onde será realizado um processo de autenticação biométrica. O sistema então poderá usar a câmera para comparar a face de Portador que está realizando as atividades do curso *online* com a imagem salva no cartão. Caso não sejam os mesmos, a pessoa não poderá realizar as atividades do curso.

Esse processo de verificação facial poderá ser contínuo, de forma que não seja possível alguma pessoa assumir o curso logo depois da primeira autenticação facial.

Em casos de avaliação onde há um agente humano monitorando pessoalmente e não houver necessidade de uma autenticação facial contínua, pode-se realizar os procedimentos apresentados na Situação 6 (Seção 4.8), onde o Portador apresenta sua identidade ao Atendente e ocorre uma autenticação biométrica do Portador.

4.1.3 Acesso a locais restritos

Em alguns casos, é necessário um controle de acesso rigoroso a certos locais em uma instituição, como laboratório ou salas de professores. Pode-se utilizar as funcionalidades que o cartão oferece para a

realização de tal tarefa.

Pode-se utilizar um cartão do Tipo 1 para, por exemplo, acesso a Restaurantes Universitários, onde apenas estudantes ligados à universidade ou à federação possuem o direito de acesso. Esse caso de uso se enquadra na Situação 1 da Seção 4.3, onde o Portador apresenta o cartão a um Atendente e este faz uma validação visual do documento para assim autorizar o Portador.

O Tipo 1 também pode ser aplicado em empréstimos de livros em biblioteca, seguindo o mesmo procedimento apresentado na Seção 4.3.

No âmbito de uma universidade, pode-se usar um cartão do Tipo 3, Tipo 4 ou Tipo 5 para um controle de acesso mais rigoroso, como por exemplo em locais onde apenas professores ou alguns estudantes possuem acesso.

Como já dito anteriormente, os cartões do Tipo 3 são para instituições que não tem recursos para documentos do Tipo 4 e 5, mas que necessitam que suas identidades sejam assinadas e possuam biometria de forma segura. Com isso, a instituição emissora poderá trabalhar com controle de acesso verificando a assinatura dos dados salvos ou com a biometria, como por exemplo, em locais onde apenas alguns usuários estão autorizados a acessar. Estes casos seguem os procedimentos apresentados na Seção 4.12 e Seção 4.13, Procedimentos 10 e 11.

Ainda citando como exemplo um local restrito, temos o Procedimento 8, descrito na Seção 4.10 onde o Portador insere o cartão em um leitor *Smart Card* e insere sua impressão digital. O sistema então fará a verificação de assinatura e a validação da impressão digital apresentada e assim autorizar o acesso.

Se não houver uma necessidade de autenticação biométrica, pode realizar o Procedimento 9, apresentado na Seção 4.11, onde há apenas uma verificação de assinatura dos dados salvos no cartão para assim ser liberado o acesso.

4.1.4 Emissão de Certificados Digitais

Conforme apresentado na Figura 10, há no cartão um campo denominado Campos de Autorização. Neste campo, uma instituição poderá armazenar certificados de atributos, conforme já descrito anteriormente.

Este campo também pode ser utilizado para armazenar certifica-

dos digitais emitidos por outras instituições de forma automática. Esse processo consiste na geração de uma requisição de certificado extraindo as credenciais de usuário do cartão. O emissor do certificado pode então realizar uma verificação no provedor de Identidade para comprovar que é um cartão de identificação válido, ou apenas verificar a assinatura dos dados presentes no circuito sem contato, para casos em que não há uma conexão com o Provedor. Esse caso se aplica para os documentos do Tipo 4 e Tipo 5.

A entidade emissora pode optar por emitir certificados de curta validade que podem ser utilizados, por exemplo, para acesso a redes sem fio em conferências em outras instituições.

Uma outra opção é a emissão de certificados para aplicações mais clássicas, como autenticação de estudantes e professores em sistemas acadêmicos.

4.2 AVALIAÇÃO DO CARTÃO DE IDENTIFICAÇÃO

Nesta seção descreve-se onze situações de uso do cartão de identificação, onde será levado em consideração os tipos do documento, a conexão com um Provedor de Identidade e quais entidades que participam do procedimento.

A Situação 1 descreve procedimentos para os casos onde há apenas um Atendente sem equipamento algum. A Situação 2 descreve procedimentos para os casos onde o Atendente possui apenas um Leitor OCR/*QR Code*. A Situação 3 descreve procedimentos para os casos onde o Atendente possui apenas um leitor *Smartcard* com contato ou sem contato.

A Situação 4 descreve procedimentos onde o Atendente possui em mãos um leitor OCR/*QR Code* e um leitor *Smartcard* com contato ou sem Contato. Já na Situação 5, descreve-se procedimentos para casos onde há todas as entidades, com exceção do Atendente.

Na Situação 6, são descritos procedimentos para casos em que o Atendente possui um Leitor de *Smartcard* com ou sem contato e um leitor de impressão digital. Já na Situação 7, há a adição do Leitor OCR/*QR Code*.

Na Situação 8, são descritos procedimentos em que há apenas o Leitor *Smartcard* com/sem Contato, leitor de impressão digital e uma Câmera. A Situação 9 descreve os procedimentos para os casos em que há apenas um Leitor *Smartcard* com ou sem contato e um leitor de impressão digital. Na Situação 10 será demonstrado procedimentos

onde há apenas um Leitor OCR/*QR Code*. E por fim, na Situação 11 há procedimentos em que há, em adição a Situação 10, um Leitor de impressão digital.

4.2.1 Tipos de Cartões de Identificação

Os Tipos de cartões já foram previamente descritos na Seção 3.4. Abaixo descreve-se resumidamente os cinco tipos propostos:

- Tipo 1: Apenas a Zona de Inspeção Visual;
- Tipo 2: Zona de Inspeção Visual com Zona Legível por Máquina;
- Tipo 3: Zona de Inspeção Visual com Zona Legível por Máquina e biometria segura;
- Tipo 4: Total funcionalidade;
- Tipo 5: Total funcionalidade com circuito sem contato.

4.2.2 Entidades participantes

Diversas entidades participam de cada situação. A seguir descreve-se cada uma delas.

4.2.2.1 Portador

O Portador é a entidade que possui o cartão de identificação em mãos e que deseja acessar algum serviço ou local. Basicamente o Portador apresenta seu documento ao Atendente que realizará todo o processo ou, em casos que não há o Atendente, o Portador realizará todo os procedimentos de apresentar o cartão para as outras entidades participantes. O Portador estará presente em todas as situações.

4.2.2.2 Atendente

O Atendente é uma entidade humana que está presente nos procedimentos de validação do cartão de identificação. Seu objetivo é realizar tarefas como a validação visual do documento e a realização de procedimentos onde há uma interação com as outras entidades não-humanas. Nos procedimentos que serão apresentados considera-se que o agente Atendente terá plenos poderes em autorizar o acesso do Porta-

dor a um determinado recurso ou local, mesmo quando este não tenha autorização para tal.

4.2.2.3 Leitor OCR/QR Code

O Leitor OCR/*QR Code* é utilizado para leitura dos dados presentes na Zona Legível por Máquina, *QR Code* e código de barras 2D. Isto pode ser feito pelo Portador do cartão ou pelo Atendente, dependendo do cenário.

4.2.2.4 Leitor Smartcard

O Leitor *Smartcard* é utilizado para ler os dados armazenados no circuito integrado do cartão de identificação. Este leitor pode utilizado tanto para leitura com contato onde é necessário inserir o cartão (cartão Tipo 4), quanto para leitura sem contato onde basta a aproximação do cartão (cartão Tipo 5). Isto pode ser feito pelo Portador do documento ou pelo Atendente, dependendo do cenário.

4.2.2.5 Leitor de impressão Digital

Utilizada para leitura da impressão digital do Portador do cartão. Após a leitura é feita uma comparação da digital que foi inserida na leitora pelo Portador com a digital armazenada no circuito integrado do cartão ou com a digital armazenada no *QR Code*. Isto pode ser feito pelo Portador do documento ou pelo Atendente, dependendo do cenário.

4.2.2.6 Câmera

Utilizada em conjunto com Leitor de *Smartcard* para realização de uma comparação visual da face do usuário com a fotografia impressa no cartão. Isto pode ser feito pelo Portador do cartão de identificação ou pelo Atendente, dependendo do cenário.

4.3 SITUAÇÃO 1

Nessa primeira situação, conforme descrito na Tabela 1, há apenas um agente humano denominado Atendente que irá realizar todo o procedimento de validação. Os diagramas de sequência das Figuras 14 e 15 ilustram os procedimentos para essa situação. Esse procedimento poderá ser aplicado a todos os tipos de cartões de identificação, uma vez que é verificado apenas os dados impressos no cartão

Tabela 1 – Entidades presentes na Situação 1.

Entidade	
Atendente	✓
Leitor OCR/QR Code	×
Leitor de *Smartcard* com/sem Contato	×
Leitor de impressão Digital	×
Câmera	×

4.3.1 Procedimento 1.1

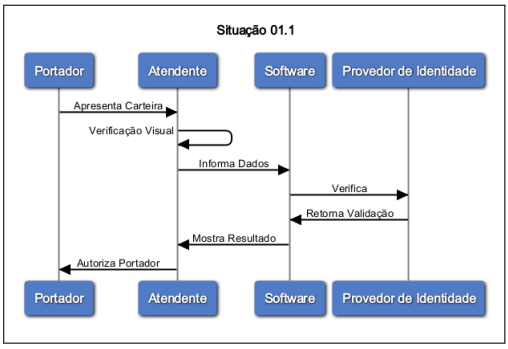

Figura 14 – Situação 1.1.

Nessa situação, o Portador apresenta seu cartão a um atendente de algum estabelecimento e havendo uma conexão com o Provedor de Identidade, o atendente pode, através de um *software* previamente con-

figurado e após uma verificação visual, realizar uma verificação no provedor e constatar se o Portador do cartão está vinculado à uma instituição participante da federação.

4.3.2 Procedimento 1.2

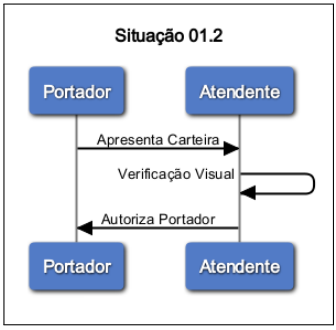

Figura 15 – Situação 1.2.

Já nessa situação, o Portador apresenta seu cartão a um atendente de algum estabelecimento e não havendo uma conexão com o Provedor de Identidade, fica a critério do atendente autorizar ou não o Portador presente através de uma validação visual.

4.3.3 Possíveis Problemas de Segurança

Nas duas situações, algumas questões de segurança devem ser observadas. Primeiro, o cartão pode ter sido falsificada. Uma vez que não há uma verificação da assinatura digital presente no chip sem contato, a parte impressa do cartão pode ter sido alterada ou até mesmo forjada. O cartão pode ter sido alterada ou forjada de forma que apenas os dados que direcionam ao Provedor de Identidade e o número de matrícula sejam verdadeiros de modo que o provedor retorne sempre como Verdadeiro uma consulta. Esse cenário se agrava mais no diagrama da Figura 15, onde não há qualquer verificação no provedor de identidade e a única coisa que um impostor deve fazer é criar um cartão de identificação com todas as características originais, incluindo por exemplo o selo da universidade.

Além disso, pode ocorrer um problema de má fé, podendo o atendente estar ciente do cartão ser falso e mesmo assim autorizar o Portador.

Este procedimento simples pode ser aplicado em cenários onde o acesso a algum lugar ou serviço não é tão restrito, como em catracas de cinema ou acesso a bibliotecas.

4.4 SITUAÇÃO 2

Nessa situação temos além do Atendente, um leitor OCR/QR Code, conforme podemos observar na Tabela 2. As Figuras 16 e 17 mostram o procedimento para quando há e quando não há uma conexão com o Provedor de Identidade. Esse procedimento pode ser aplicado a todos os tipos de cartões, com excessão do Tipo 1.

Tabela 2 – Entidades presentes na Situação 2.

Entidade	
Atendente	✓
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	×
Leitor de impressão Digital	×
Câmera	×

4.4.1 Procedimento 2.1

Esse procedimento é bem similar ao apresentado na Seção 4.3, com adição da leitora OCR/QR Code. Nessa situação, o atendente usa a leitora para ler os dados do cartão e enviar para algum *software*. Este por sua vez irá realizar uma validação no Provedor de Identidade (se disponível) identificado no cartão. O atendente irá então autorizar ou não o Portador a ter acesso a algum recurso ou local, dependendo do retorno da Provedor de Identidade.

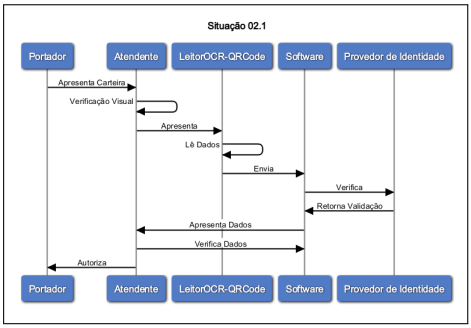

Figura 16 – Situação 2.1.

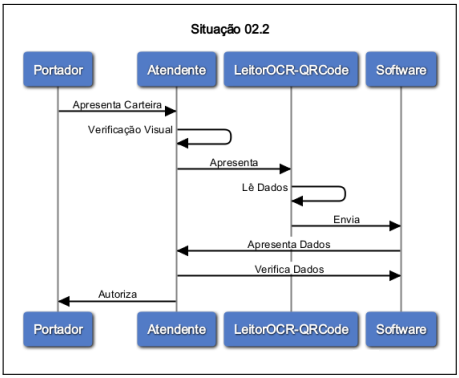

Figura 17 – Situação 2.2.

4.4.2 Procedimento 2.2

Nessa situação não há uma conexão com um Provedor de Identidade, então fica a cargo do atendente autorizar ou não o Portador (para os cartões do Tipo 1). Para os cartões do Tipo 2, 3, 4 e 5, o Atendente pode utilizar o Leitor para ler o código de barras do cartão e assim verificar a assinatura dos dados impressos no cartão.

4.4.3 Possíveis Problemas de Segurança

Os mesmos problemas apresentados na Seção 4.3.3 se aplicam nessa situação para os cartões do Tipo 1. Há também o risco de um Portador mal intencionado conseguir de alguma forma alterar a foto, nome e data de nascimento de um cartão válido, tanto do VIZ quanto do MRZ, ou imprimir um cartão com essas características. Esse cartão possuirá dados de validação que serão aceitos no provedor de identidade, fazendo com que a validação visual e a validação do provedor de identidade sejam verdadeiras.

4.5 SITUAÇÃO 3

Nessa situação, onde os integrantes são apresentados na Tabela 3, o Atendente possuirá apenas um leitor *Smart Card* em mãos, que poderá ser usado para a leitura dos dados do circuito sem contato presente no cartão. Este procedimento pode ser aplicado nos cartões do Tipo 4 e 5.

Tabela 3 – Entidades presentes na Situação 3.

Entidade	
Atendente	✓
Leitor OCR/QR Code	×
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	×
Câmera	×

4.5.1 Situação 3.1

Na situação apresentada na Figura 18, o Portador apresenta o cartão ao Atendente, que após uma validação visual insere o cartão em uma leitora de *smart cards*. Após o atendente inserir o cartão na leitora, será solicitado a partir de um *software* alguns dados para a geração de chave de acesso aos grupos de dados do circuito. O Atendente irá, então, inserir esses dados e os dados do cartão serão extraídos e apresentados na tela de um computador, onde o Atendente realizará uma verificação,

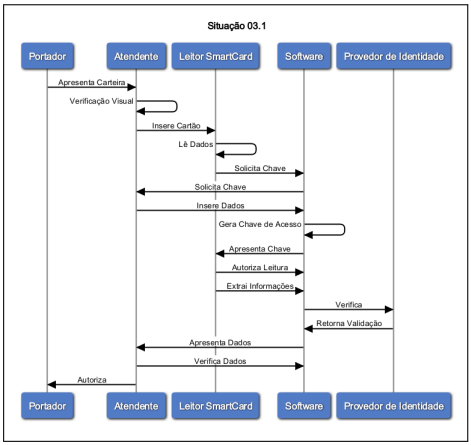

Figura 18 – Situação 3.1.

enquanto o *software* verifica no Provedor de Identidade se o usuário é válido ou não. Após o retorno da validação por parte do Provedor de Identidade, o atendente autoriza o Portador a acessar o serviço ou local controlado.

4.5.2 Situação 3.2

Esta situação é muito semelhante à situação 3.1 na seção 4.5.1. Entretanto, aqui não há a conexão com o Provedor de Identidade. Assim, após inserir o cartão na leitora e inserir os dados necessários, o atendente verificará os dados apresentados na tela de seu computador e o *software* verificará a assinatura armazenada no circuito integrado. Caso esteja tudo certo, o Portador estará autorizado a acessar algum serviço ou local controlado.

4.5.3 Possíveis Problemas de Segurança

Nessa situação o maior problema de segurança está relacionado com o Atendente, que mesmo constatando após todo o procedimento que o cartão apresentado não pertence ao Portador presente, o Atendente pode autorizar o acesso agindo de má fé e prejudicando a segu-

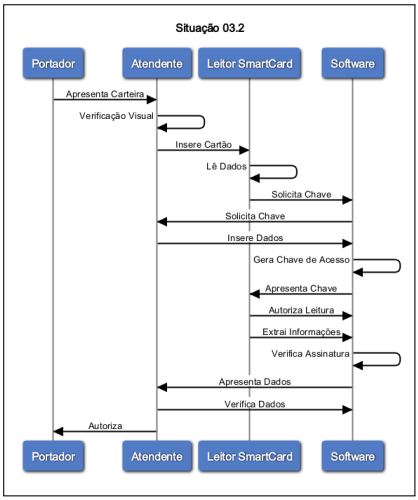

Figura 19 – Situação 3.2.

rança.

Uma forma de resolver isso seria não dar poderes ao Atendente de liberar o acesso ao serviço ou local que o Portador deseja acessar. Assim, somente aqueles com cartões válidos e autorizados poderiam conseguir o acesso ao que precisam, ficando ao Atendente somente a função de monitorar as ações dos Portadores.

4.6 SITUAÇÃO 4

Nessa situação, onde além dos participantes já existentes na situação anterior, temos em adição um leitor OCR/QR Code, conforme podemos observar na tabela 4. Este procedimento pode ser aplicado nos cartões do Tipo 2 ao 5.

4.6.1 Situação 4.1

Nesta situação, o atendente, após a validação visual e antes de inserir o cartão em uma leitora, usa o leitor QR Code/OCR para ler os dados impressos no MRZ ou no QR Code que são salvos em um *software*. Também é possível, nesse passo, o sistema verificar a assina-

Tabela 4 – Entidades presentes na Situação 4.

Entidade	
Atendente	✓
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	×
Câmera	×

tura para os Tipos 2, 3, 4 e 5. Em seguida, insere o cartão na leitora onde os dados do circuito integrado são lidos e demonstrados na tela do computador utilizado. O *software* então faz a validação no Provedor de Identidade. Caso o retorno da validação no Provedor seja verdadeira, então o atendente autoriza o Portador. A Figura 20 mostra o procedimento.

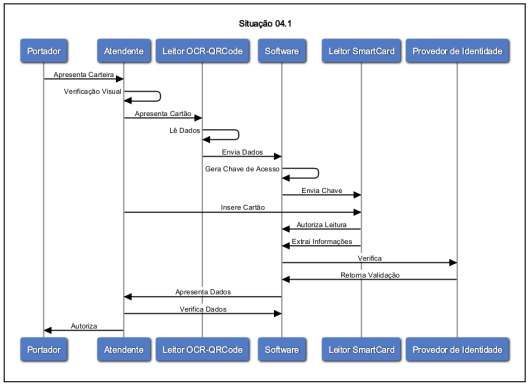

Figura 20 – Situação 4.1.

4.6.2 Situação 4.2

Observa-se nesta situação um procedimento similar ao anterior. Entretanto, sem uma conexão com o Provedor de Identidade. Assim após os passos de validação visual e leitura do *QR Code*/MRZ, o atendente verifica os dados que serão apresentados no *software* e este, por sua vez faz uma verificação *offline* dos dados do cartão: como não há uma conexão com o Provedor de Identidade, será verificado se os dados assinados digitalmente são verdadeiros ou se não foram alterados. Tendo adquirido anteriormente a chave que foi utilizada para assinar os dados no cartão e o utilizando para verificar a assinatura, se esta for válida o atendente poderá liberar o Portador. Este procedimento poderá ser observado na Figura 21.

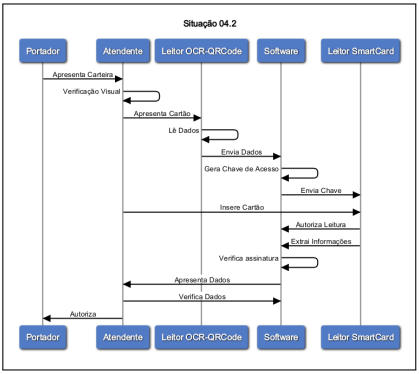

Figura 21 – Situação 4.2.

4.6.3 Possíveis Problemas de Segurança

Assim como na Situação 3 na Seção 4.5.3, o maior problema de segurança é o próprio Atendente. Mesmo constatando após todo o procedimento de que o cartão apresentado não pertence ao Portador presente, o Atendente pode autorizar o acesso.

Assim como na Situação 3, uma forma de resolver isso seria não dar poderes ao Atendente de liberar o acesso quando o mesmo desejar. Assim somente aqueles com cartões válidos e autorizados poderiam conseguir o acesso ao que precisam, ficando ao Atendente somente a função de monitorar as ações dos Portadores.

4.7 SITUAÇÃO 5

Nesta situação, todos os equipamentos farão parte dos procedimentos com exceção do agente humano (Atendente), conforme demonstrado na Tabela 5. Assim, todo o procedimento deverá ser realizado pelo próprio Portador do cartão. Importante ressaltar que terá acesso à biometria salva no cartão apenas entidades autorizadas pelo emissor do cartão. Este procedimento se aplica nos cartões do Tipo 3 ao 5.

Tabela 5 – Entidades presentes na Situação 5.

Entidade	
Atendente	×
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	✓
Câmera	✓

4.7.1 Situação 5.1

Nesta situação o Portador do cartão deseja acessar um local com acesso controlado: somente membros da federação possuem o acesso e é necessário uma autenticação biométrica para o Portador ter a permissão de acessar o local. A Figura 22 descreve o procedimento. O Portador apresenta o cartão a um leitor OCR/QR Code que lê os dados impressos

no cartão e os envia para um *software* que realizará o processo de geração de chave para o acesso aos dados do circuito sem contato.

Após essa leitura o Portador irá aproximar ou inserir o cartão em uma leitora *smartcard*, onde o *software* irá apresentar a chave gerada e fazer a leitura dos dados salvos no circuito integrado e enfim, realizar uma verificação no Provedor de Identidade. Caso o Provedor retorne uma validação Verdadeira, o processo de autenticação do Portador continuará, caso contrário, o Portador não será autorizado a acessar o local.

Com o retorno verdadeiro, será solicitado ao usuário uma leitura biométrica onde o Portador aproximará um de seus dedos no leitor biométrico para que seja feita uma leitura biométrica. Caso a digital apresentada seja equivalente a digital salva no circuito integrado, o procedimento segue em frente.

Por fim é feita uma validação visual através da câmera. Se a validação for verdadeira, o Portador estará autorizado.

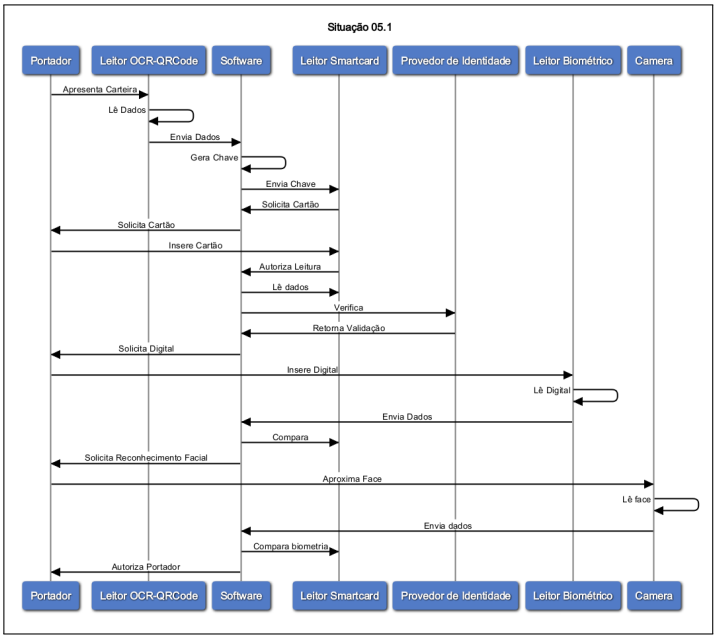

Figura 22 – Situação 5.1.

4.7.2 Situação 5.2

Nessa situação não há uma conexão com o Provedor de Identidade, seja por realmente não haver uma conexão ou por não ser necessário. Conforme mostrado na Figura 23, ocorre um procedimento parecido com o anterior. Assim, o Portador realizará os mesmos procedimentos e o *software* irá verificar as assinaturas digitais salvas no circuito integrado. Tendo adquirido anteriormente o certificado que foi utilizado para assinar os dados no cartão e o utilizando para verificar a assinatura, o sistema então autorizará ou não o acesso do Portador.

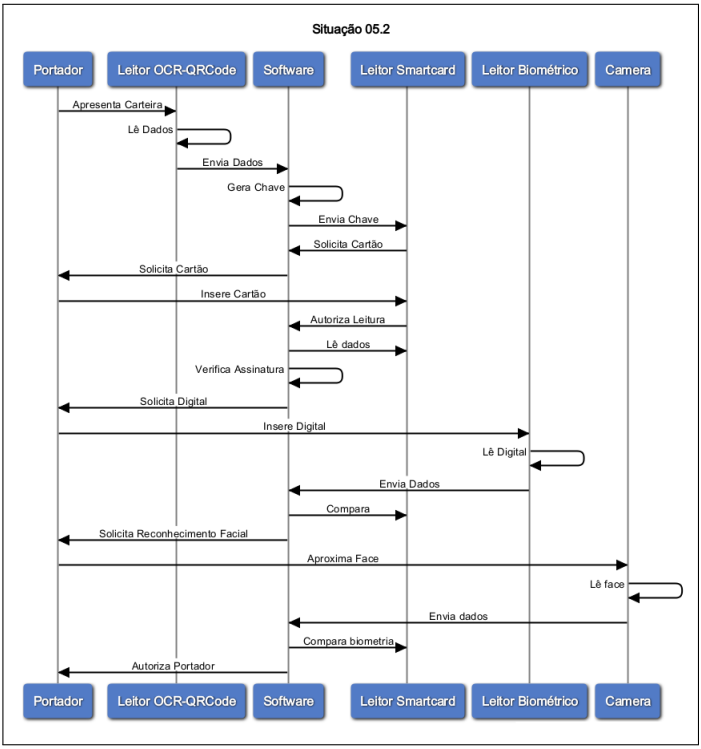

Figura 23 – Situação 5.2.

4.7.3 Possíveis Problemas de Segurança

Nessa situação o próprio dispositivo para leitura biométrica pode estar suscetível a algum tipo de ataque. Conforme apresentado em Ratha, Connell e Bolle (2001), um usuário mal intencionado, como por exemplo um usuário com um cartão roubado, pode de alguma forma apresentar ao leitor uma digital forjada. Essa digital pode ser equivalente àquela armazenada no circuito sem contato, e uma vez que não tem-se o Atendente para verificar o que o Portador está apresentando no leitor, este obterá o acesso.

Portanto, é necessário que a Leitora Biométrica possua mecanismos de segurança para evitar que problemas como esse ocorram.

Além disso, pode haver problemas na questão da revogação de credenciais, onde um portador apresenta um cartão com informações e biometrias válidas mas revogada pelo emissor. Não havendo conexão com um provedor de Identidade o sistema não poderá realizar essa verificação.

4.8 SITUAÇÃO 6

Nesta situação, há um Atendente juntamente com um leitor *Smart Card* e um leitor biométrico. Neste cenário não está disponível o leitor OCR/QR Code e nem a câmera. A Tabela 6 demonstra os participantes nessa situação. Importante ressaltar que terá acesso à biometria salva no cartão somente Entidades autorizadas pelo emissor do cartão. Este procedimento se aplica nos cartões do Tipo 4 e 5.

Tabela 6 – Entidades presentes na Situação 6.

Entidade	
Atendente	✓
Leitor OCR/QR Code	×
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	✓
Câmera	×

4.8.1 Situação 6.1

Nesta situação, o Portador apresenta o cartão ao Atendente que realiza uma validação visual. Se o cartão for válido, o atendente insere ou aproxima o cartão na leitora *Smart Card* e insere manualmente em um *software* os dados necessários para a geração da chave para leitura do conteúdo presente no circuito integrado. O sistema, então, gera a chave e realiza a leitura dos dados.

Em seguida, o sistema realizará uma verificação no Provedor de Identidade e o mesmo retornará a validação. Caso o retorno do provedor seja válido, o atendente solicitará que o Portador insira sua digital no leitor biométrico para a verificação. Se a digital inserida pelo Portador coincidir com a digital do cartão, a validação seguirá em frente. Caso contrário, o Portador não será autorizado.

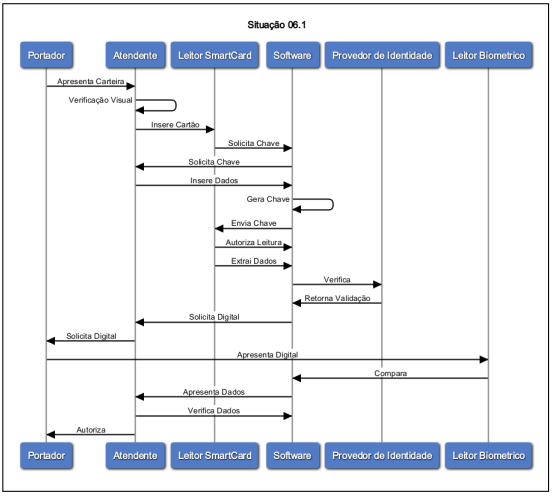

Figura 24 – Situação 6.1.

4.8.2 Situação 6.2

Esta situação é similar à situação anterior, entretanto como não há uma conexão com o Provedor de Identidade, o sistema verifica as assinaturas presentes no documento. Esse procedimento é detalhado

na Figura 25.

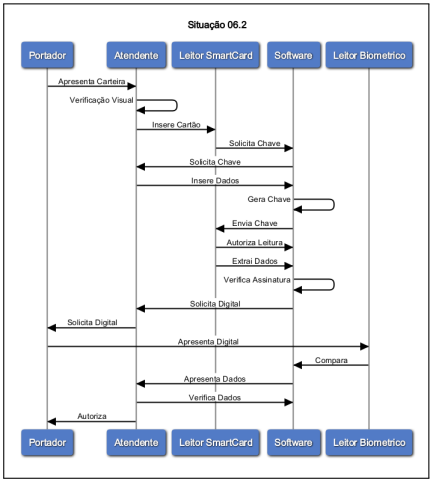

Figura 25 – Situação 6.2.

4.8.3 Possíveis Problemas de Segurança

Assim como na Situação 3 e 4 nas Seções 4.5.3 e 4.6.3, o maior problema de segurança é o próprio Atendente. Mesmo constatando após todo o procedimento de que o cartão apresentado não pertence ao Portador presente. A forma de resolver isso seria não dar poderes ao Atendente de liberar o acesso quando o mesmo desejar. Assim somente aqueles com cartões válidos e autorizados poderiam conseguir o acesso ao que precisam, ficando ao Atendente somente a função de monitorar as ações dos Portadores.

4.9 SITUAÇÃO 7

Nesta situação, o Atendente tem a disposição todos os equipamentos necessários com exceção da Câmera, conforme podemos observar na Tabela 7. Este procedimento de aplica nos cartões do Tipo 4 e 5.

Tabela 7 – Entidades presentes na Situação 7.

Entidade	
Atendente	✓
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	✓
Câmera	×

4.9.1 Situação 7.1

Nesta situação, o Portador apresenta seu cartão ao Atendente que realiza uma inspeção visual, comparando a foto impressa com o Portador. Feito isso, o atendente realiza a leitura dos dados presentes no MRZ ou do QR Code e os envia para um *software*. Com os dados lidos, é inserido ou aproximado o cartão no leitor *smartcard*.

O *software* então gera uma chave com os dados lidos no MRZ ou QR Code para obter acesso aos dados do circuito integrado para logo depois ler os dados e realizar uma verificação no Provedor de Identidade. Caso o retorno do Provedor seja Verdadeiro, então a verificação continua, caso contrário o Portador não será autorizado a ter acesso ao o que deseja.

Então, após a validação no Provedor de Identidade, o atendente solicita ao Portador que insira sua digital. O sistema então lê a digital e compara com a digital presentes no cartão. Se a comparação for falsa, o Portador não estará autorizado a seguir em frente.

4.9.2 Situação 7.2

Nesta situação temos todos os passos da situação anterior, entretanto não temos uma conexão com um Provedor de Identidade. Com isso após a validação visual do Atendente e leitura do QR Code ou MRZ e antes das comparações dos dados biométricos, o sistema verifica se os dados presentes no circuito integrado não foram alterados e, tendo obtido anteriormente o certificado de assinatura, também verifica se o cartão foi emitido por uma universidade que faz parte de uma determinada federação.

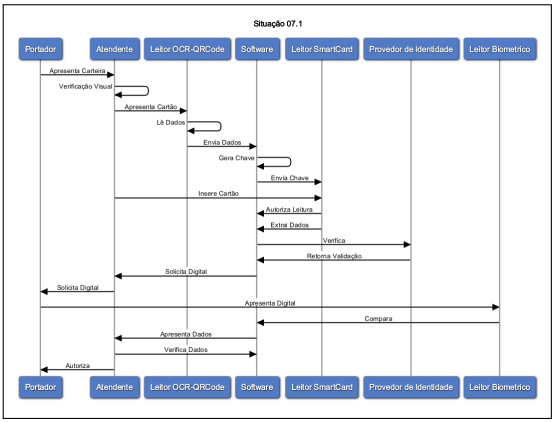

Figura 26 – Situação 7.1.

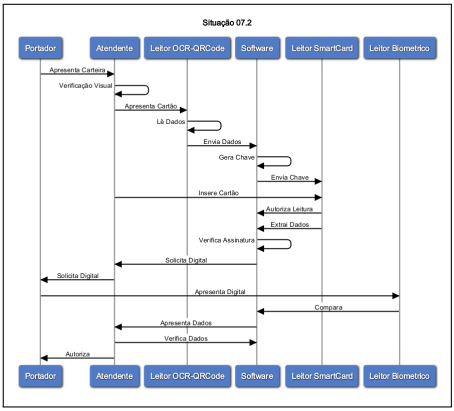

Figura 27 – Situação 7.2.

4.9.3 Possíveis Problemas de Segurança

Assim como na Situação 3, 4 e 6 nas Seções 4.5.3. 4.6.3 e 4.8.3 o maior problema de segurança é o próprio Atendente. A solução é a mesma apresentada para esses casos.

4.10 SITUAÇÃO 8

Nesta situação, não há o Atendente, e também não há um leitor QR Code ou OCR. Consequentemente, o Portador terá que informar manualmente os dados para a geração da chave de acesso. Os participantes nessa situação podem ser visualizados na Tabela 8. Este procedimento pode ser aplicado nos cartões do Tipo 4 e 5.

Tabela 8 – Entidades presentes na Situação 8.

Entidade	
Atendente	×
Leitor OCR/QR Code	×
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	✓
Câmera	✓

4.10.1 Situação 8.1

Como não há um leitor QR Code ou OCR e também não há o Atendente, será o Portador que fará todo o trabalho. Então após o usuário inserir seu cartão em uma leitora, o sistema solicitará os dados necessários para geração da chave. O Portador então informará os dados necessários a partir de um teclado. O sistema verificará se o cartão apresentado é válido no Provedor de Identidade equivalente. Caso o retorno do Provedor for inválido, não será autorizado o acesso do usuário.

Se o retorno for válido, o sistema solicitará ao Portador a impressão digital e a aproximação da câmera para reconhecimento facial. O sistema compara esses dados com os dados salvos no circuito digital. Se os dados são equivalentes, o sistema, então, autoriza o acesso ao usuário, caso contrário, não será autorizado.

4.10.2 Situação 8.2

Nesta situação, como não há a conexão com o Provedor de Identidade, o próprio sistema verificará a consistência dos dados salvos no

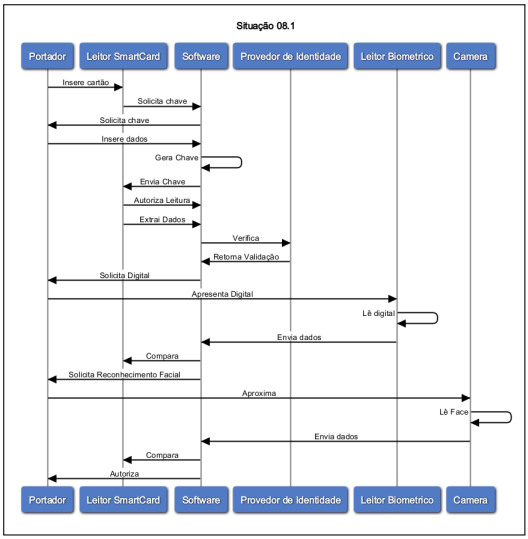

Figura 28 – Situação 8.1.

circuito integrado, utilizando o certificado utilizado na emissão o cartão. Caso algum dado tenha sido alterado anteriormente, ou se o cartão não foi emitida por uma instituição participante de uma federação ou se nem sequer foi emitido por uma instituição, o usuário não será autorizado a prosseguir. A Figura 29 demonstra esse procedimento.

4.10.3 Possíveis Problemas de Segurança

Em ambos os procedimentos, não havendo um agente humano para uma verificação visual, um Portador com um cartão válido poderá liberar uma catraca de uma biblioteca por exemplo, e após a liberação deixa outra pessoa ter acesso ao local.

4.11 SITUAÇÃO 9

Essa situação é uma das mais simples. Aqui não temos um Atendente e equipamentos de leitura de dados biométricos, conforme apresentado na Tabela 9. Este procedimento se aplica nos cartões do Tipo

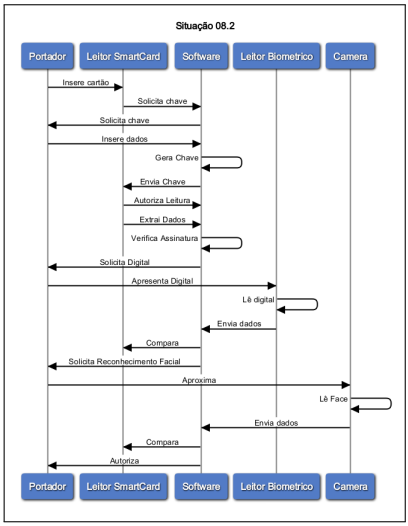

Figura 29 – Situação 8.2.

4 e 5.

Tabela 9 – Entidades presentes na Situação 9.

Entidade	
Atendente	×
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	✓
Leitor de impressão Digital	×
Câmera	×

4.11.1 Situação 9.1

Primeiramente o usuário apresenta seu cartão a um leitor OCR ou QR Code para que o sistema leia os dados impressos. Em seguida o Portador insere ou aproxima o cartão em uma leitora *smartcard* para que seja lido os dados do circuito integrado. Paralelamente a isso, o sistema gera a chave de acesso para a leitura dos dados e em seguida lê

os dados e realiza a verificação necessária no Provedor de Identidade. Caso o retorno seja válido, o sistema autoriza o acesso ao usuário.

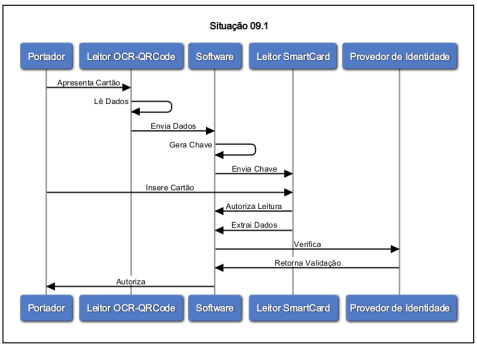

Figura 30 – Situação 9.1.

4.11.2 Situação 9.2

Aqui não há uma conexão com o Provedor de Identidade, assim a única coisa que o sistema poderá fazer é verificar se os dados salvos no circuito integrado não foram alterados ou se realmente foi emitido por uma instituição de uma federação válida, através de uma verificação de assinatura.

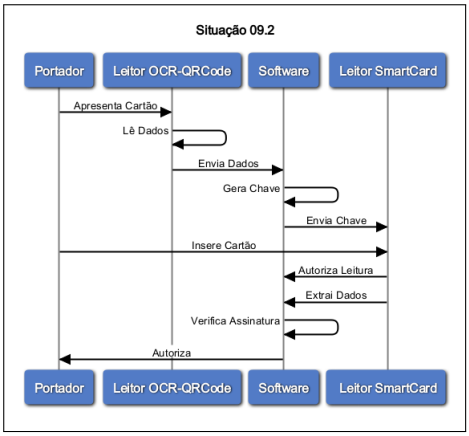

Figura 31 – Situação 9.2.

4.11.3 Possíveis Problemas de Segurança

Assim como no Situação 8 na Seção 4.10, não há um Atendente para monitoras as ações do Portador presente. Assim, um Portador mal intencionado pode apenas usar seu cartão para a liberação do acesso e, posteriormente, permitir que outras pessoas entrem no local, mesmo que estas não estejam autorizadas.

4.12 SITUAÇÃO 10

Essa situação também é simples. Aqui não há um Atendente e equipamentos de leitura de dados biométricos, conforme apresentado na Tabela 10. Temos apenas um leitor OCR/*QR Code*. Este procedimento se aplica nos cartões que possuem *QR Code*.

4.12.1 Situação 10.1

Nesta situação o Portador apresenta o *QR Code* ao leitor, onde este irá realizar a leitura dos dados e verificar se a assinatura salva no código é válida ou não. Caso a assinatura seja válida, então o sistema autorização o Portador. Este procedimento pode ser observado

Tabela 10 – Entidades presentes na Situação 10.

Entidade	
Atendente	×
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	×
Leitor de impressão Digital	×
Câmera	×

na Figura 32.

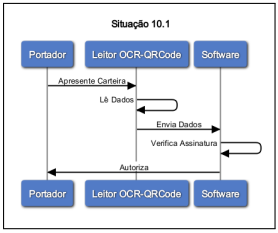

Figura 32 – Situação 10.1.

4.12.2 Possíveis Problemas de Segurança

Assim como no Situação 9 na Seção 4.11, não há um Atendente para monitoras as ações do Portador presente. Assim, um Portador mal intencionado pode apenas usar seu cartão para a liberação do acesso e permitir que outras pessoas entrem no local.

4.13 SITUAÇÃO 11

Nesta situação, há apenas um OCR/*QR Code* e uma leitora biométrica onde é feita uma comparação da digital armazenada no *QR Code* com a digital do Portador. Este procedimento se aplica somente no Tipo 3.

Tabela 11 – Entidades presentes na Situação 11.

Entidade	
Atendente	×
Leitor OCR/QR Code	✓
Leitor de *Smartcard* com/sem Contato	×
Leitor de impressão Digital	✓
Câmera	×

4.13.1 Situação 11.1

Nesta situação o Portador apresenta o *QR Code* ao leitor, onde este irá realizar a leitura dos dados e verificar se a assinatura salva no código (cartão Tipo 3) é válida ou não. Após a validação, o sistema solicita ao Portador que apresente sua digital e compara a digital salva no *QR Code* com a digital impressa. Caso a biometria seja equivalente, o Portador estará autorizado. Este procedimento pode ser observado na Figura 33.

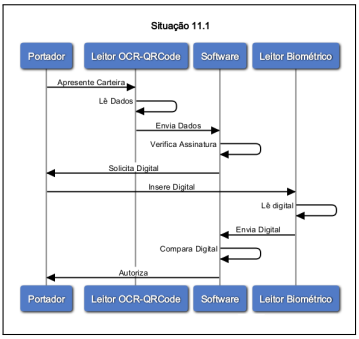

Figura 33 – Situação 11.1.

4.13.2 Possíveis Problemas de Segurança

Assim como no Situação 10 na Seção 4.12, não há um Atendente para monitorar as ações do Portador presente, o Portador mal intencionado pode usar seu cartão para a liberação do acesso e permitir que outras pessoas entrem no local, mesmo que estas não estejam autorizadas.

4.14 CONSIDERAÇÕES SOBRE CAPÍTULO

Neste capítulo foi descrito uma proposta de cartão de identificação baseado na documentação ICAO 9303 que pode ser utilizado no âmbito das federações. Também foi apresentado diversos exemplos de aplicações do cartão em diversos ambientes.

Além disso, foi realizado uma validação de segurança da proposta apresentada, levando em consideração as entidades participantes e a infraestrutura utilizada. Com essa validação através de diagramas de sequência foi possível identificar alguns possíveis problemas de segurança e como resolve-los. Com isso foi possível também identificar qual o cenário mais seguro que pode ser utilizado, que é o cenário apresentado Situação 7, Seção 4.9, onde há a presença de todas as entidades, com excessão da Câmera que é desnecessária aqui, devido a presença do Atendente. Nessa situação além da Autenticação Biométrica e validação dos dados salvos no circuito integrado, há a presença do Atendente para validação visual do cartão de identificação e também para a rea-

lização do procedimento.

5 CONCLUSÕES E TRABALHOS FUTUROS

Nesta dissertação foi apresentada uma proposta de Cartão de Identificação baseado nas especificações dos documentos de viagem. O cartão foi pensado para que qualquer instituição possa emitir seu documento de identificação, podendo ainda ser utilizado no âmbito de federações de identidade.

No âmbito de tais federações, o cartão resolve alguns dos problemas descritos anteriormente. Um dos problemas apresentados é que as Federações requerem que provedores de serviços e identidades estejam disponíveis *online*, ou seja, o provedor de identidade e a instituição de origem precisam de alguma forma se comunicarem para que os usuários possam acessar algum serviço. É possível utilizar a proposta apresentada para a realização de autenticação de forma que não é preciso uma conexão com a Internet, uma vez que diversos dados estão impressos e armazenados no circuito integrado do cartão de forma segura e assinados pela instituição emissora.

Outro problema levantado é que as identidades providas por Federações de Identidade requerem o uso de computadores para sua verificação, restringindo seu uso ao contexto dos sistemas computacionais, dificultando a verificação por agentes humanos. O cartão aqui descrito permite que seja realizada esta autenticação por agentes humanos, através dos dados impressos no cartão. Tal ação é útil em casos onde a identificação é necessária e ordinária, como em descontos em cinemas e teatros.

Além desses, uma outra importante questão é que alguns dados são considerados privados, confidenciais e de uso restrito. Neste sentido, a instituição de origem não pode compartilhá-los através de seu provedor de identidade, pois, caso ocorra seu vazamento, a instituição pode sofrer sanções legais por quebra de privacidade. O cartão proposto nessa dissertação permite que o portador carregue de forma segura suas credenciais de autenticação, como dados biométricos, que são armazenados de forma segura no circuito integrado e assinados, onde somente instituições autorizadas tem acesso à biometria armazenada. Assim, não haverá necessidade destes dados serem transmitidos através da rede mundial de computadores.

Em adição, foi realizado uma avaliação de segurança da proposta apresentada. Essa avaliação foi realizada na forma de cerimônias utilizando digramas de sequência. Nessa avaliação foi levado em consideração diversos cenários, sendo possível identificar problemas de segurança

que podem ocorrer em cada caso, e descrito formas de resolver tais problemas. Além disso foi descrito diversos exemplos de uso do cartão de identificação, relacionando-os com as cerimônias apresentadas.

Como trabalhos futuros, sugere-se a implementação de um sistema federado para coleta de credenciais e emissão automatizada de cartões. Esse sistema pode ser primeiramente implementado em instituições de ensino participantes de federações de identidade acadêmicas. Nessa situação um usuário ligado à instituição deve se apresentar a um ponto de emissão onde o sistema verificará seus dados e emitirá o cartão.

Pode ser desenvolvido um Diretório de Chaves Púbicas (PKD) para todas as instituições participantes de uma determinada Federação de Identidade. Esse diretório contém as chaves públicas de cada instituição participante. Assim quando é necessária uma verificação de assinaturas, pode-se consultar o diretório para obter-se a chave pública correspondente do emissor do cartão e assim realizar os procedimentos de validação.

Uma outra sugestão de trabalho futuro seria a adaptação do cartão de identificação para dispositivos móveis, onde os dados de identificação e dados biométricos ficam armazenadas de forma segura em um dispositivo como um *smartphone*. Isso poderá ser opcional para cada instituição e até mesmo para o Usuário final que poderá ter a opção de salvar os dados em seu dispositivo ao invés da emissão de um cartão, diminuindo os custos para a instituição emissora.

A implementação do *Match on card* para biometria também é sugerido como trabalho futuro. Com isso, a autenticação biométrica é feita no cartão e não há uma extração dos dados biográficos, evitando assim a clonagem de tais dados. Em adição, pode-se realizar a implementação de um modelo biométrico para cifragem de biometria nos cartões do Tipo 3 para evitar roubo de biometria apenas lendo o *QR Code*.

E por fim sugere-se a carga de credenciais no formato de certificados de atributos. Pode-se usar certificados de atributos privados com Prova de Conhecimento Zero, onde o portador prova que suas credenciais são verdadeiras sem entretanto apresentar as mesmas.

REFERÊNCIAS

AHN, G.-J.; LAM, J. Managing privacy preferences for federated identity management. In: *Proceedings of the 2005 Workshop on Digital Identity Management*. New York, NY, USA: ACM, 2005. (DIM '05), p. 28–36. ISBN 1-59593-232-1. <http://doi.acm.org/10.1145/1102486.1102492>.

AHN, G.-J.; SHIN, D.; HONG, S.-P. Information assurance in federated identity management: Experimentations and issues. In: ZHOU, X. et al. (Ed.). *Web Information Systems – WISE 2004*. Springer Berlin Heidelberg, 2004, (Lecture Notes in Computer Science, v. 3306). p. 78–89. ISBN 978-3-540-23894-2. <http://dx.doi.org/10.1007/978-3-540-30480-7$_1$0>.

AUSTRALIAN ACCESS FEDERATION. *About Australian Access Federation*. 2014. Acesso em 2014-09-04. <http://aaf.edu.au/about/>.

BALDONI, R. Federated identity management systems in e-government: the case of italy. *EG*, v. 9, n. 1, p. 64–84, 2012. <http://dblp.uni-trier.de/db/journals/eg/eg9.htmlBaldoni12>.

BARROS, A.; LEHFELD, N. de S. *Fundamentos de metodologia: um guia para a iniciação científica*. São Paulo: MAKRON, 2007. 158 p.

BERTINO, E. et al. Standards for web services security. In: *Security for Web Services and Service-Oriented Architectures*. Springer Berlin Heidelberg, 2010. p. 45–77. ISBN 978-3-540-87741-7. <http://dx.doi.org/10.1007/978-3-540-87742-4$_4$>.

BHARGAV-SPANTZEL, A. et al. User centricity: A taxonomy and open issues. *J. Comput. Secur.*, IOS Press, Amsterdam, The Netherlands, v. 15, n. 5, p. 493–527, out. 2007. ISSN 0926-227X. <http://dl.acm.org/citation.cfm?id=1370624.1370625>.

BHARGAV-SPANTZEL, A.; SQUICCIARINI, A. C.; BERTINO, E. Establishing and protecting digital identity in federation systems. In: *Proceedings of the 2005 Workshop on Digital Identity Management*. New York, NY, USA: ACM, 2005. (DIM '05), p. 11–19. ISBN 1-59593-232-1. <http://doi.acm.org/10.1145/1102486.1102489>.

CANE, P.; CONAGHAN, J. *The New Oxford Companion to Law*. [S.l.]: Oxford University Press, 2008. 1306 p. (Oxford Companions Series).

CASCIANI, D. *Analysis: The first ID cards*. [S.l.], sep 2008. Disponível em: <http://news.bbc.co.uk/2/hi/uk_news/politics/7634744.stm>. Acesso em: 5 sep. 2014.

CHADWICK, D. Federated identity management. In: ALDINI, A.; BARTHE, G.; GORRIERI, R. (Ed.). *Foundations of Security Analysis and Design V*. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, v. 5705). p. 96–120. ISBN 978-3-642-03828-0. <http://dx.doi.org/10.1007/978-3-642-03829-7$_3$>.

COCK, D. D.; WOLF, C.; PRENEEL, B. The belgian electronic identity card (overview). In: *Sicherheit 2006: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI), 20.-22. Februar 2006 in Magdeburg*. [s.n.], 2006. p. 298–301. <http://subs.emis.de/LNI/Proceedings/Proceedings77/article4522.html>.

DONALD, J. *Chambers's Etymological Dictionary of the English Language*. [S.l.]: W. and R. Chambers, 1867. 583 p.

EDUGATE. *About Edugate*. [S.l.], jul 2014. Disponível em: <http://www.edugate.ie/content/about-us>. Acesso em: 5 jul. 2014.

FEDERAL MINISTRY OF INTERIOR. *Electronic Identification with the New German National Identity Card*. 2014. Acesso em 2014-09-04. <http://www.personalausweisportal.de/EN/Citizens/Electronic-Identification/Electronic-Identification_node.html>.

FEDERAL MINISTRY OF INTERIOR. *Neue Anwendung für die Online-Ausweisfunktion*. 2014. Acesso em 2014-09-04. <http://www.personalausweisportal.de/DE/Home/home_node.html>.

FEDERAL OFFICE FOR INFORMATION SECURITY. *Security mechanisms in electronic ID documents*. [S.l.], jul 2015. Disponível em: <http://tinyurl.com/zncdp46>. Acesso em: 28 jul. 2015.

GLASSER, U.; VAJIHOLLAHI, M. Identity management architecture. In: *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*. [S.l.: s.n.], 2008. p. 137–144.

GLOBO. *Unificação de documentos no Brasil fica na promessa*. [S.l.], jan 2014. Disponível em: <http://glo.bo/1lLJSvO>. Acesso em: 18 dec. 2015.

HAGGARD, S. *The Maturing of the MOOC*. Department for Business, Innovation and Skills, 2013. Acesso em 2014-09-04. <http://tinyurl.com/nv89lyr>.

HAN, J. et al. A generic construction of dynamic single sign-on with strong security. In: JAJODIA, S.; ZHOU, J. (Ed.). *Security and Privacy in Communication Networks*. Springer Berlin Heidelberg, 2010, (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, v. 50). p. 181–198. ISBN 978-3-642-16160-5. <http://dx.doi.org/10.1007/978-3-642-16161-$2_1$1>.

ICAO. *Part 3 - Machine Readable Official Travel Documents. Volume 1 - MRtds with Machine Readable Data Stored in Optical Character Recognition Format*. Third. [S.l.], 2008. Acesso em 2014-09-04. <http://www.icao.int/publications/Documents/9303_p3_v1_cons_en.pdf>.

ICAO. *Part 3 - Machine Readable Official Travel Documents. Volume 2 - Specifications for Electronically Enabled MRtds with Biometric Identification Capability*. 2008. Acesso em 2014-09-04. <http://www.icao.int/publications/Documents/9303_p3_v2_cons_en.pdf>.

ICAO. *MRTD History*. 2014. Acesso em 2014-09-04. <http://www.icao.int/Security/mrtd/Pages/MRTDHistory.aspx>.

ICAO. *Part 11 - Security Mechanisms for MRTDs*. Seventh. [S.l.], 2015. Acesso em 2015-08-29. <http://www.icao.int/publications/Documents/9303_p11_cons_en.pdf>.

IDEM. *About IDEM*. [S.l.], jul 2014. Disponível em: <https://www.idem.garr.it/en/about>. Acesso em: 5 jul. 2014.

INCOMMON. *About InCommon*. [S.l.], jul 2014. Disponível em: <http://www.incommon.org/about.html>. Acesso em: 5 jul. 2014.

ISIC. *About ISIC*. [S.l.], jul 2014. Disponível em: <http://www.isic.org/about-us/>. Acesso em: 5 sep. 2014.

ISIC. *O que é a Carteira Mundial do Estudante*. 2014. Acesso em 2014-09-04. <http://www.carteiradoestudante.com.br/saiba-tudo-carteira-mundial.aspx>.

ISO. *Country Codes*. [S.l.], 2000. Disponível em: <http://www.iso.org/iso/country$_c$*odes* > .*Acessoem* : 18*jun*.2015.

ISO. *Information technology - Automatic identification and data capture techniques - QR Code bar code symbology*. [S.l.], 2000. Disponível em: <https://www.iso.org/obp/ui/iso:std:iso-iec:18004:ed-3:v1:en>. Acesso em: 18 jun. 2015.

ITU. *ITU-T X.509 (10/2012)*. [S.l.], sep 2000. Disponível em: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>. Acesso em: 5 sep. 2014.

JENSEN, J. Federated identity management challenges. In: *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*. [S.l.: s.n.], 2012. p. 230–235.

LANDAU, S.; GONG, H. L. V.; WILTON, R. Achieving privacy in a federated identity management system. In: DINGLEDINE, R.; GOLLE, P. (Ed.). *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, v. 5628). p. 51–70. ISBN 978-3-642-03548-7. <http://dx.doi.org/10.1007/978-3-642-03549-4_4>.

LIBERTY-ALLIANCE. *Liberty ID-FF Architecture Overview*. [S.l.], jan 2003. Disponível em: <https://www.oasis-open.org/committees/download.php/4329/liberty-idff-arch-overview-v1.2.pdf>. Acesso em: 5 jul. 2014.

MADSEN, P.; KOGA, Y.; TAKAHASHI, K. Federated identity management for protecting users from id theft. In: *Proceedings of the 2005 Workshop on Digital Identity Management*. New York, NY, USA: ACM, 2005. (DIM '05), p. 77–83. ISBN 1-59593-232-1. <http://doi.acm.org/10.1145/1102486.1102500>.

MALER, E.; REED, D. The venn of identity: Options and issues in federated identity management. *Security Privacy, IEEE*, v. 6, n. 2, p. 16–23, March 2008. ISSN 1540-7993.

MICROSOFT. *Perguntas freqüentes do Microsoft Passport*. [S.l.], jan 2003. Disponível em: <http://support.microsoft.com/kb/277759/pt-br>. Acesso em: 5 oct. 2014.

MINISTERO DELL'INTERNO. *Carta d'identità elettronica - Cie*. 2014. Acesso em 2014-09-04.

<http://www.interno.gov.it/mininterno/site/it/temi/servizi_demografici/scheda_006.html>.

MINISTERO DELL'INTERNO. *Decreto 8 novembre 2007*. 2014. Acesso em 2014-09-04. <http://www.interno.gov.it/mininterno/site/it/sezioni/servizi/legislazione/enti_locali/0997_2007_11_08_Decreto_8_novembre_2007.html>.

MOREIRA, E. Q. et al. *Federação CAFe Implantação do Provedor de Identidade*. [S.l.]: Rede Nacional de Ensino e Pesquisa, 2011.

MOSTOWSKI, W.; POLL, E. *Electronic Passports in a Nutshell*. 2010.

NIINUMA, K.; JAIN, A. K. Securing epassport system: A proposed anti-cloning and anti-skimming protocol. In: *Biometric Technology for Human Identification VII*. [S.l.: s.n.], 2010. p. 90–94.

RATHA, N. K.; CONNELL, J. H.; BOLLE, R. M. An analysis of minutiae matching strength. In: SPRINGER. *Audio-and Video-Based Biometric Person Authentication*. [S.l.], 2001. p. 223–228.

REDE NACIONAL DE ENSINO E PESQUISA. *The Federated Academic Community*. [S.l.], jul 2014. Disponível em: <http://portal.rnp.br/web/servicos/cafe-en>. Acesso em: 28 jul. 2014.

RNP. *Programa de Gestão de Identidade*. 2014. Acesso em 2016-02-29. <https://wiki.rnp.br/display/comitetgi/PGId+2014+-+Propostas+Selecionadas>.

ROSSETO, S. et al. *Federação CAFe: Implantação do Provedor de Identidade. Rio de Janeiro: Escola Superior de Redes*. [S.l.]: Escola Superior de Redes, 2014.

SAADE, D. M.; CARRANO, R. C.; SILVA, E. F. *Eduroam: Acesso sem fio seguro para a Comunidade Acadêmica Federada*. Rede Nacional de Ensino e Pesquisa, 2013. <http://www.scribd.com/doc/125531184/Eduroam-Acesso-sem-Fio-Seguro-para-Comunidade-Academica-Federada>.

SAEED, M.; MASOOD, A.; KAUSAR, F. Securing epassport system: A proposed anti-cloning and anti-skimming protocol. In: *International Conference on Software, Telecommunications Computer Networks, 2009. SoftCOM 2009. 17th*. [S.l.: s.n.], 2009. p. 90–94.

SASSO, F. C.; MORAES, R. R. D.; MARTINA, J. E. A proposal for a unified identity card for use in an academic federation environment. In: *2014 Ninth International Conference on Availability, Reliability and Security (ARES),*. [S.l.: s.n.], 2014. p. 265–272.

SHIBBOLETH. *Shibboleth*. [S.l.], sep 2014. Disponível em: <https://shibboleth.net/>. Acesso em: 5 sep. 2014.

SHIN, D.; LOPES, R.; CLAYCOMB, W. Authenticated dictionary-based attribute sharing in federated identity management. In: *Sixth International Conference on Information Technology: New Generations, 2009. ITNG '09.* [S.l.: s.n.], 2009. p. 504–509.

SPELTENS, M.; PATTERSON, P. Federated id management — tackling risk and credentialing users. In: *ISSE/SECURE 2007 Securing Electronic Business Processes*. Vieweg, 2007. p. 130–135. ISBN 978-3-8348-0346-7. <http://dx.doi.org/10.1007/978-3-8348-9418-$2_1$4>.

SQUICCIARINI, A. C.; CZESKIS, A.; BHARGAV-SPANTZEL, A. Privacy policies compliance across digital identity management systems. In: *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*. New York, NY, USA: ACM, 2008. (SPRINGL '08), p. 72–81. ISBN 978-1-60558-324-2. <http://doi.acm.org/10.1145/1503402.1503416>.

TÁVORA, R. G. F.; TORRES, J. A. S.; FUSTINONI, D. F. R. Proposta de um modelo de documento de identidade robusto a fraudes e de baixo custo. *XV Simpósio Brasileiro em Segurança da Informaçao e de Sistemas Computacionais*, p. 574–585, oct 2015.

TERENA. *About eduroam*. [S.l.], sep 2014. Disponível em: <https://www.eduroam.org/>. Acesso em: 10 sep. 2014.

TERENA. *About TERENA*. [S.l.], sep 2014. Disponível em: <http://www.terena.org/about/>. Acesso em: 10 sep. 2014.

WANGHAM, M. S. et al. Uma infraestrutura para tradução de credenciais de autenticação para federações shibboleth. *X Simpósio Brasileiro em Segurança da Informaçao e de Sistemas Computacionais*, p. 360–447, 2010.

WIERENGA, K.; FLORIO, L. Eduroam: past, present and future. In: *Computational Methods in Science and Technology*. [S.l.: s.n.], 2005. v. 11, p. 169–173.

WOLF, M. et al. A message meta model for federated authentication in service-oriented architectures. In: *Service-Oriented Computing and Applications (SOCA), 2009 IEEE International Conference on.* [S.l.: s.n.], 2009. p. 1–8.